

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**




**Overview**

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central, Firewall Rule Management and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 9,118,711 (the "'711 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '711 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

9,100,431 Claim 1	Evidence
<p>1. A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:</p>	<p>ManageEngine includes <i>a computer program product (Manage Engine) embodied on a non-transitory computer readable medium, the computer program product comprising:</i></p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p> <div data-bbox="758 553 1717 634" style="border: 2px solid red; padding: 5px; text-align: center;"> <b>Enterprise vulnerability management software</b> </div> <p style="text-align: center;">Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step <a href="#">vulnerability management</a> in your enterprise with Vulnerability Manager Plus.</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div data-bbox="722 954 961 1252" style="text-align: center;"> <p><b>Scan</b></p>  <p>Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.</p> </div> <div data-bbox="1087 954 1402 1252" style="text-align: center;"> <p><b>Assess</b></p>  <p>Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.</p> </div> <div data-bbox="1520 954 1885 1252" style="text-align: center;"> <p><b>Manage</b></p>  <p>Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.</p> </div> </div> <p><a href="https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&amp;loc=ProdMenu&amp;cat=UEMS">https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&amp;loc=ProdMenu&amp;cat=UEMS</a></p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Comprehensive vulnerability scanning</b></p> <p>Eliminating blind spots is the basis of successful <b>vulnerability management</b>. To achieve this, Vulnerability Manager Plus:</p> <ul style="list-style-type: none"> <li>• Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.</li> <li>• Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.</li> <li>• Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.</li> </ul> <p><a href="https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html">https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html</a></p>
<p>code for allowing access to first information from at least one first data storage identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability;</p>	<p>ManageEngine includes a <i>code for allowing access to first information from at least one first data storage</i> (e.g., information present in the Central Vulnerability Database) <i>identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability</i> (e.g., vulnerability data present in the Central Vulnerability Database);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**2) What is Vulnerability Scanning?**

Vulnerability scanning is a security process that checks your computer systems to find any weaknesses or vulnerabilities that could be used by hackers to gain unauthorized access. It's like a thorough check-up for your network and software, where any potential security risks are identified and reported back to you so that you can take action to fix them. This helps to protect your organization's digital assets and ensures that sensitive information remains secure.

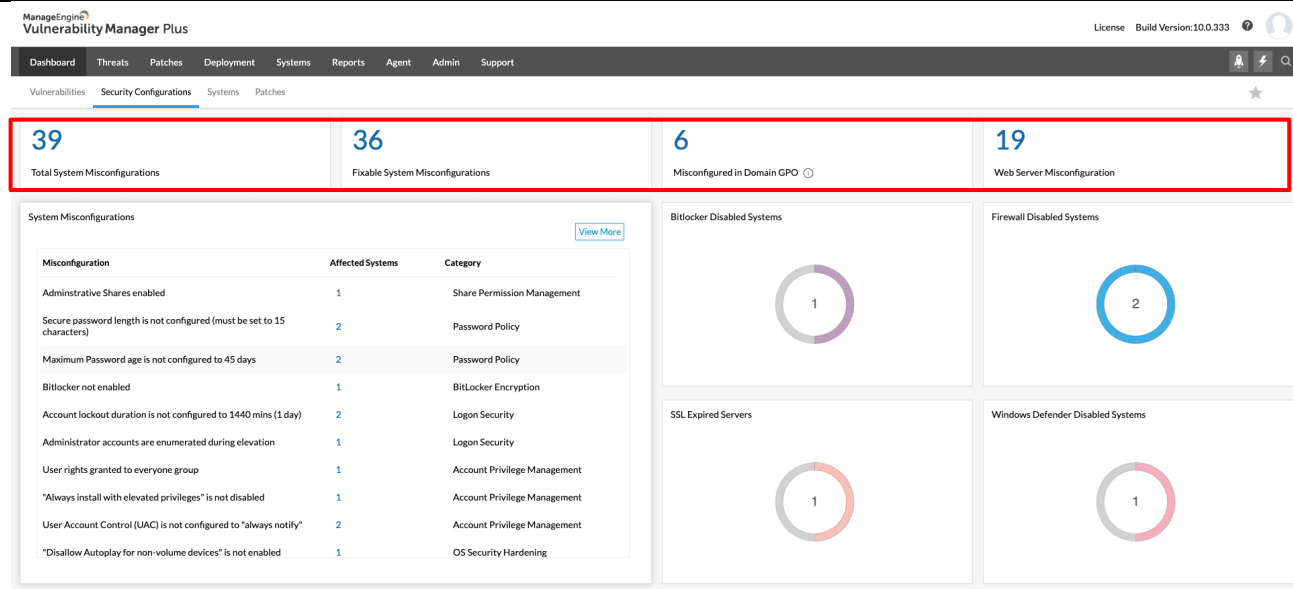
<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

**Comprehensive vulnerability scanning**

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:


- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>


**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>


**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar lists various threat categories, with 'Zero-day Vulnerabilities' highlighted. The main panel displays a table of zero-day vulnerabilities. The table has columns for Threats, Threat Category, Affected Systems, and Action. The data rows show specific vulnerabilities like Google Chrome (x64) (78.0.3904.87) and various Internet Explorer security updates, each with a 'Fix' button. A search bar at the top allows filtering by CVE ID. The bottom right shows pagination: '1 - 5 of 5' and '30'.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

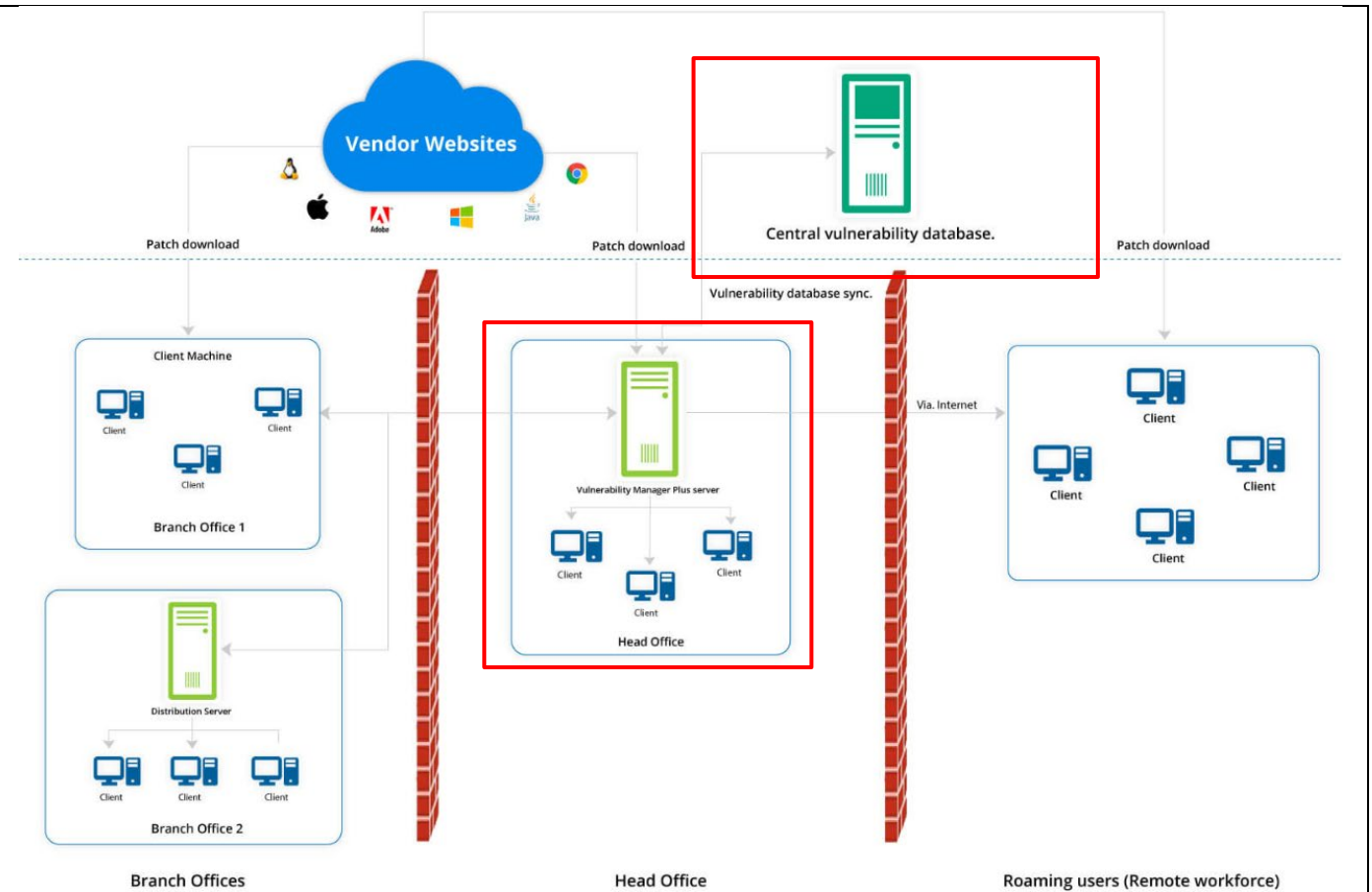
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the *Vulnerability Manager Plus* pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****See what matters most at a glimpse with dashboard widgets**





The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
SummaryZero-day  
vulnerabilitiesVulnerability  
Age MatrixVulnerabilities  
Over Time**High Priority  
Vulnerabilities****High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

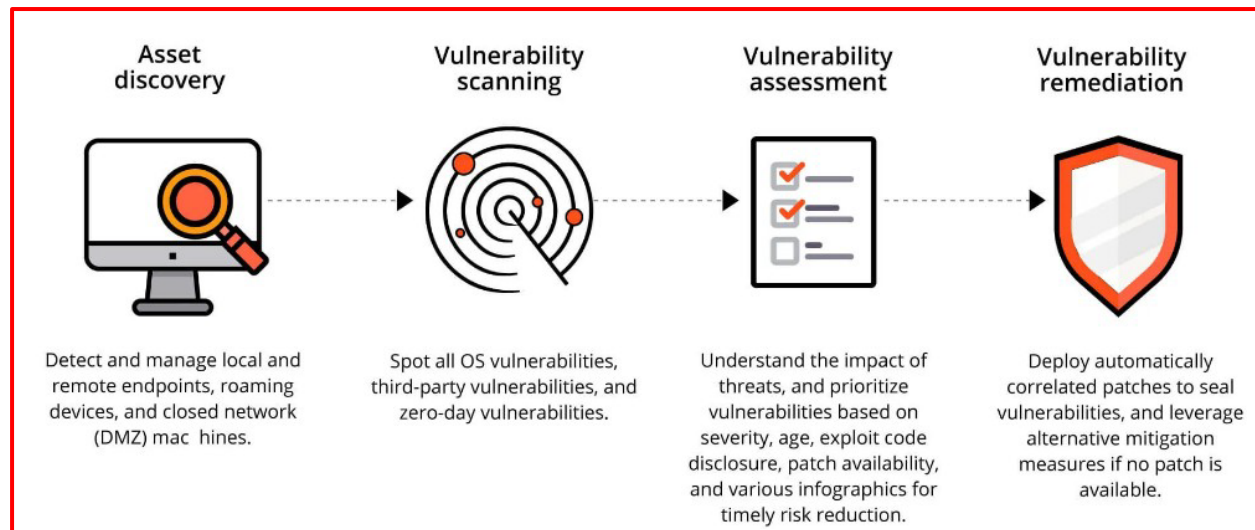
<p>code for causing at least one operation in connection with at least one of a plurality of networked devices, the at least one operation configured for:</p> <p>identifying at least one configuration associated with the at least one networked device, and</p> <p>determining that the at least one networked device is actually vulnerable to one or more actual vulnerabilities, based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities, such that second information is</p>	<p>ManageEngine includes a <i>code for causing at least one operation in connection with at least one of a plurality of networked devices</i> (e.g., scanning operation performed on any part of the endpoints (network devices) of the architecture), <i>the at least one operation configured for: identifying at least one configuration associated with the at least one networked device</i> (e.g., run scans on the vulnerability so that the vulnerability can be identified), <i>and determining that the at least one networked device is actually vulnerable to one or more actual vulnerabilities</i> (e.g., known/existent vulnerabilities to the devices), <i>based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities</i> (e.g., unknown/potential vulnerabilities to the devices), <i>such that second information is stored in at least one second data storage</i> (e.g., data storage on network devices or other means to view network storage device vulnerability details) <i>separate from the at least one first data storage, the second information identifying the one or more actual vulnerabilities to which the at least one networked device is actually vulnerable;</i></p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>
---	---

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

stored in at least one second data storage separate from the at least one first data storage, the second information identifying the one or more actual vulnerabilities to which the at least one networked device is actually vulnerable;

### What are the 4 steps in vulnerability assessment?

Vulnerability Manager Plus is a well-rounded vulnerability assessment tool that regularly scans your network for vulnerabilities, delivers insights into risk, and helps close the vulnerability management loop instantly with direct remediation from the console.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot displays the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar shows a navigation menu with options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'Threats' and includes a sub-header: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this, there is a filter section with 'Filter by: Threat Categ...' and a search bar 'Search by CVE ID: CVE-XXXX-XXXX'. A table lists several threats, including Google Chrome (x64) (78.0.3904.87) and various Internet Explorer security updates. The table columns are Threats, Threat Category, Affected Systems, and Action. The bottom of the table shows '1 - 5 of 5' and a pagination control.

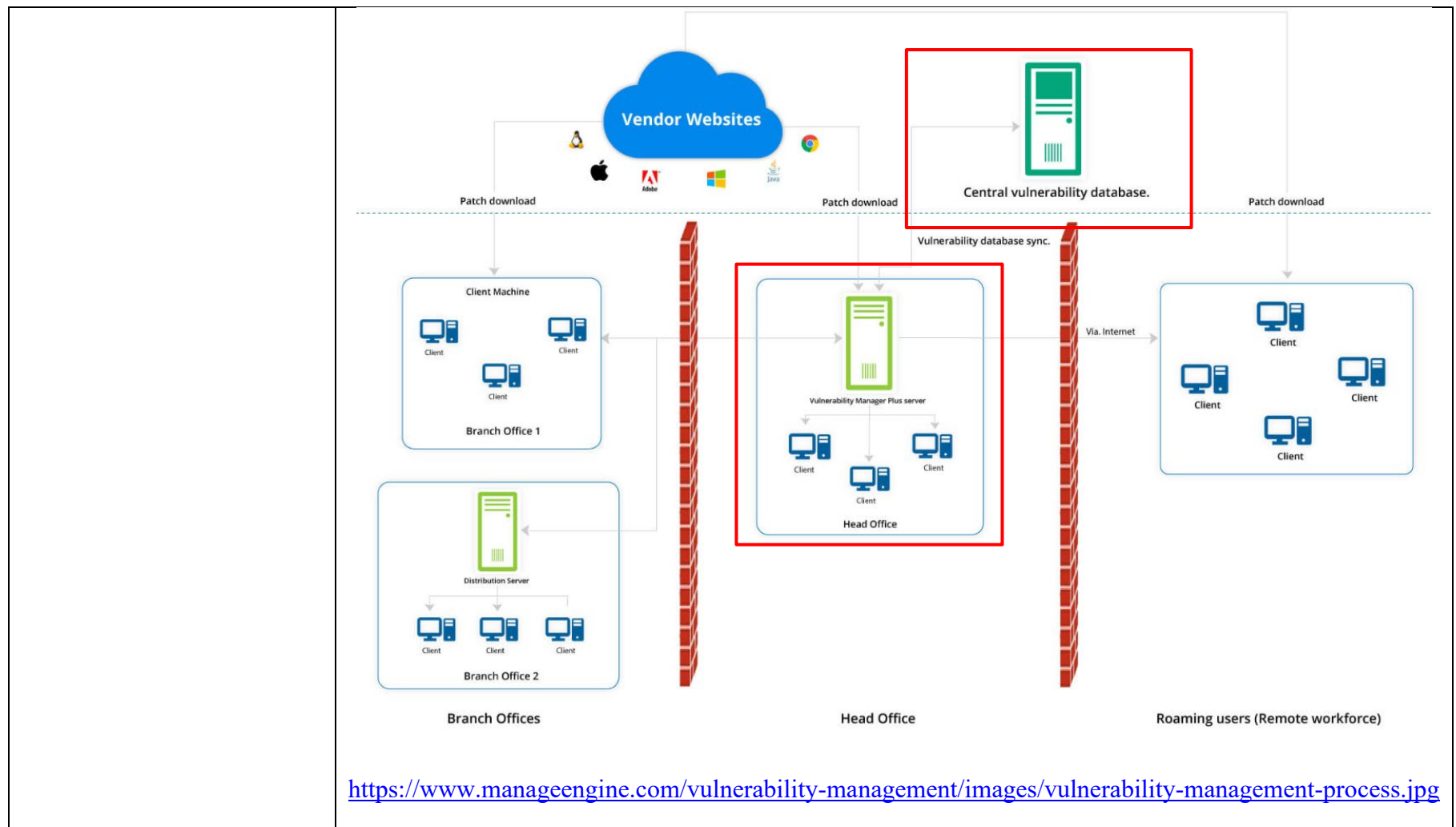
Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network. Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the *Vulnerability Manager Plus* pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

### High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

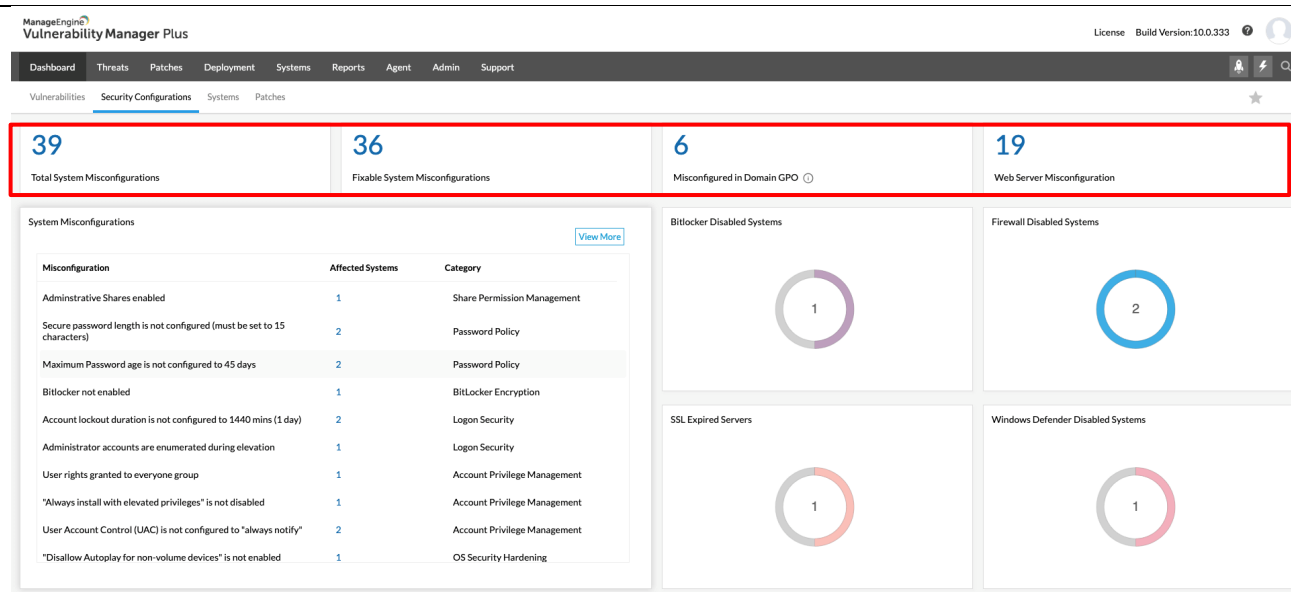
Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

code for identifying a first occurrence in connection with the at least one networked device and a second occurrence in connection with the at least one networked device;

ManageEngine includes a *code for identifying a first occurrence in connection with the at least one networked device and a second occurrence in connection with the at least one networked device* (e.g., the first and second events of detection of a vulnerability wherein the occurrences can identify different vulnerabilities);

**Note:** See, for example, the evidence below (emphasis added, if any):

### **| Comprehensive vulnerability scanning**

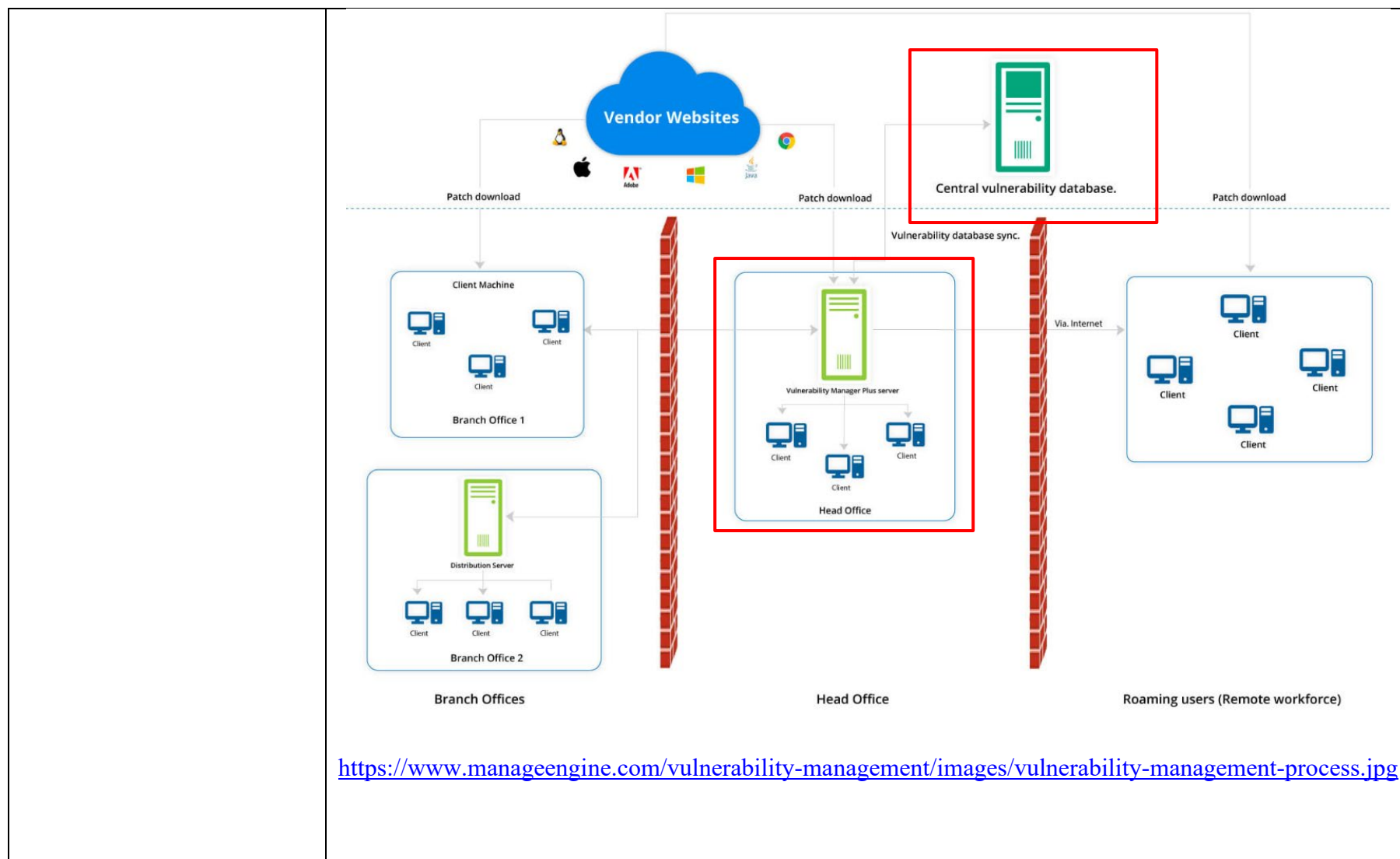
Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Other features</b></p> <div> <div> <p><b>Firewall Reports</b></p> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div> <p><b>Firewall Log Management</b></p> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div> <p><b>Firewall Alerts</b></p> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div> <p><b>Firewall Compliance Management</b></p> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div> <p><b>Real-time Bandwidth Monitoring</b></p> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div> <p><b>Manage Firewall Service</b></p> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> </div> <p><a href="https://www.manageengine.com/products/firewall/firewall-rule-management.html">https://www.manageengine.com/products/firewall/firewall-rule-management.html</a></p>
code for: determining the first occurrence to have a first severity if the at least one networked device is actually	ManageEngine includes a <i>code for: determining the first occurrence to have a first severity</i> (e.g., a threat level of the vulnerability i.e., critical, important, moderate, and low) <i>if the at least one networked device is actually vulnerable to at least one of the actual vulnerabilities that is capable of being taken advantage of by the first occurrence identified in connection with the at least one networked device, and further</i>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

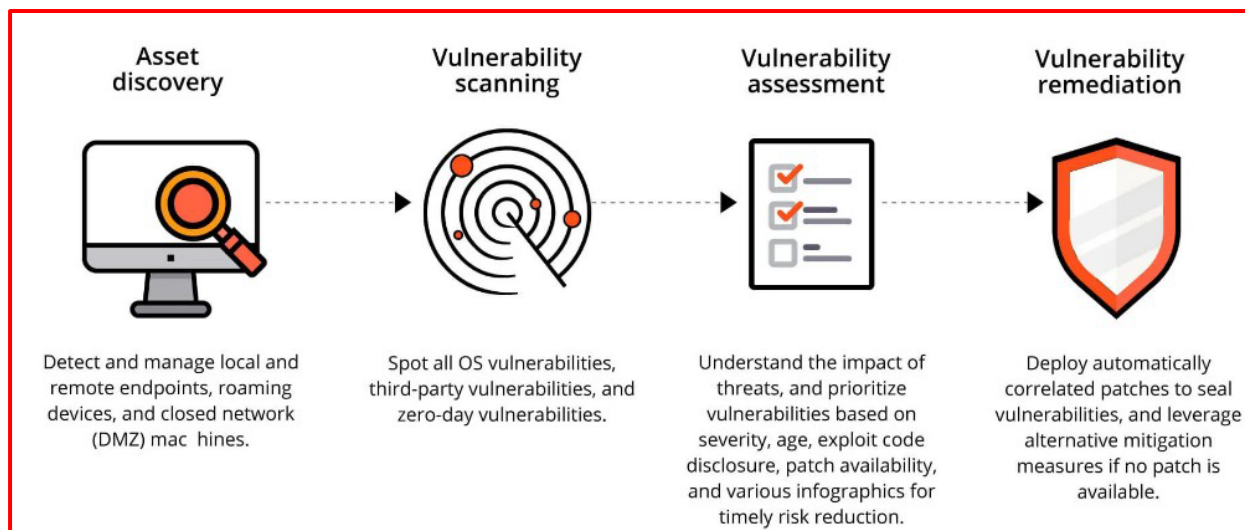
vulnerable to at least one of the actual vulnerabilities that is capable of being taken advantage of by the first occurrence identified in connection with the at least one networked device, and further determining the second occurrence to have a second severity if the at least one networked device is not actually vulnerable to the second occurrence identified in connection with the at least one networked device;

*determining the second occurrence to have a second severity (e.g., a threat level of the vulnerability i.e., critical, important, moderate, and low) if the at least one networked device is not actually vulnerable to the second occurrence identified in connection with the at least one networked device;*

**Note:** See, for example, the evidence below (emphasis added, if any):

### What are the 4 steps in vulnerability assessment?

Vulnerability Manager Plus is a well-rounded vulnerability assessment tool that regularly scans your network for vulnerabilities, delivers insights into risk, and helps close the vulnerability management loop instantly with direct remediation from the console.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

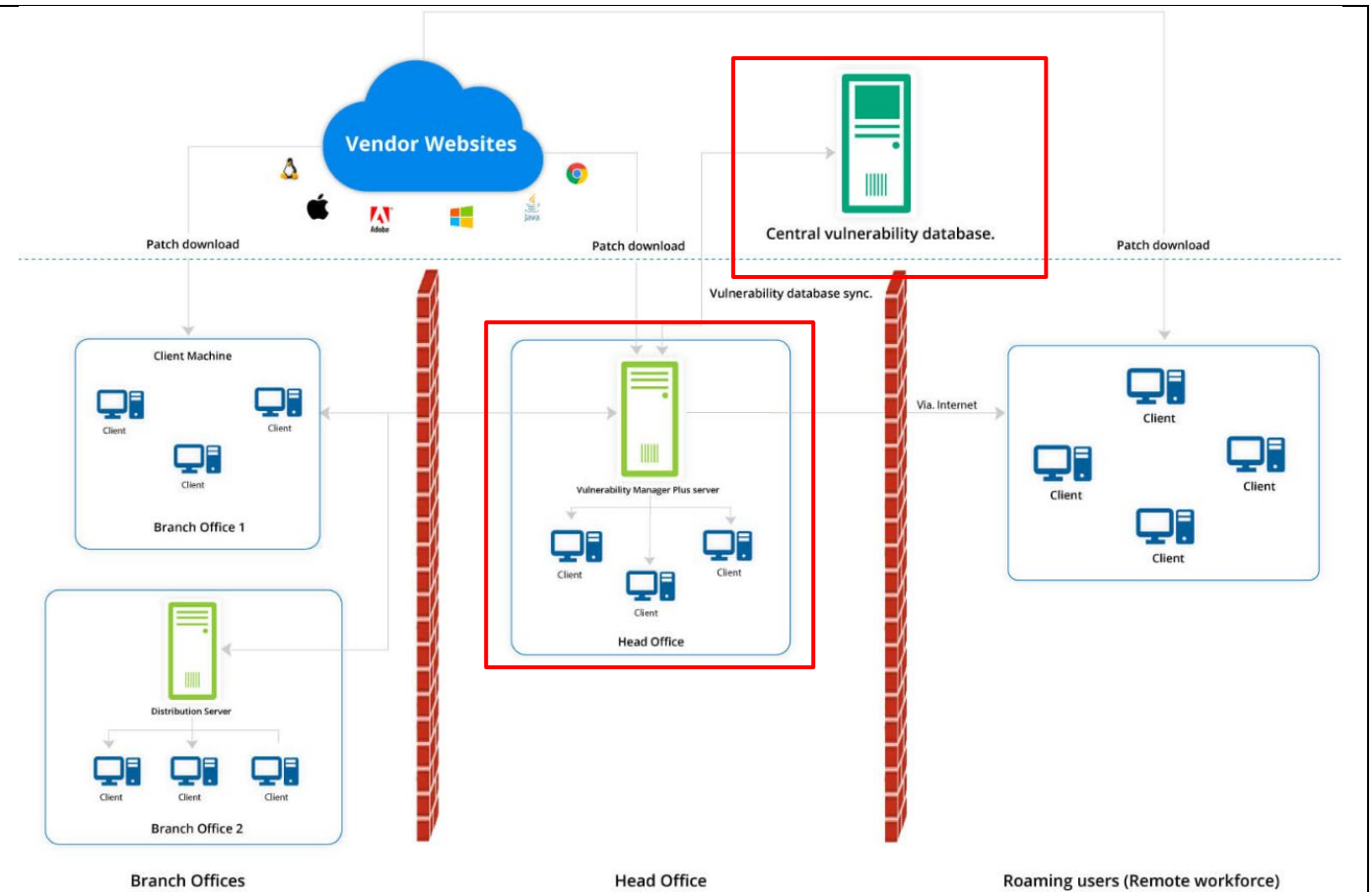
**Assessing software vulnerabilities:**

Vulnerability Manager Plus regularly scans your network for vulnerabilities. Once vulnerabilities are detected, then they are displayed in the web console. New vulnerabilities are being discovered constantly, therefore, it might get overwhelming for an user to decide on which vulnerability to remediate first. Therefore vulnerabilities should be assessed and prioritized based on the risk it presents to the enterprise. Vulnerability Manager Plus helps you assess the risk posed by vulnerabilities with the help of following parameters:

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Severity levels:**

Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability.

**Critical:**

Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first.

**Important:**

Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers.

**Moderate:**

Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS).

**Low:**

Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited.

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

code for reporting the first occurrence and the second occurrence differently based on the first severity and the second severity;

ManageEngine includes a *code for reporting the first occurrence and the second occurrence differently based on the first severity and the second severity* (e.g., the critical severities and the important severities are reported immediately to the user, and any severity requiring immediate actions from a user are reported immediately wherein the moderate and low type of severities are either not reported by solving through automated patches or sent via a periodic report either generated automatically or on user's request);

**Note:** See, for example, the evidence below (emphasis added, if any):

| Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

| Vulnerability Age:

Vulnerability Manager Plus lets you calculate the age of a vulnerability either from the date on which the vulnerability is published or from the date on which it is discovered in your network. Letting a vulnerability reside in your network for a longer time is an indication of weak security. Therefore, vulnerability age must be taken into consideration while prioritizing vulnerabilities.

Using the above mentioned parameters, Vulnerabilities can be assessed and prioritized in many ways depending on your needs. It is advisable to use a combination of parameters to prioritize vulnerabilities. You can perform the entire operation of [vulnerability assessment](#) and remediation directly from the Vulnerability Manager Plus console.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**| Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Manager Plus. The interface includes a sidebar with navigation options such as 'Manual Deployment', 'Test and Approve', 'Automate Patch Deployment', 'Disable Automatic Updates', 'Security Configurations', 'Software Uninstallation', 'Deployment Policies', 'Trash', 'Tools', 'Remote Shutdown', and 'Wake on LAN'. The main content area is divided into several sections:


- Name and Description:** A form to enter the patch name (e.g., 'MyConfiguration970') and an 'Add Description' link.
- Install Patch:** A section for selecting the operation type (Install Patch or Uninstall Patch) and a table of patches.
- Scheduler Settings [optional]:** Checkboxes for 'Install After' and 'Do not apply this configuration after the time specified below'.
- Deployment Rule:** A checkbox for 'Continue deployment even if some patches cannot be downloaded'.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' and a 'Create/Modify Policy' link.
- Define Targets:** A section for defining targets, including a table for 'Filter Computers based on' and 'Exclude Target'.
- Execution Settings [Optional]:** A section for defining execution settings.

This integrated vulnerability and patch management approach eliminates the need for multiple agents, disparity in data transferred between multiple solutions, potential delays in remediation, unnecessary silos, and false positives. Vulnerability Manager Plus also empowers you with a [separate patch management module](#) to completely automate your regular patching schedules, enabling your IT staff to spend more time on assessing and prioritizing high-risk vulnerabilities.


<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Severity levels:**

Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability.

**Critical:**

Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first.

**Important:**

Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers.

**Moderate:**

Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS).

**Low:**

Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited.

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Other features</b></p> <div> <div> <p><b>Firewall Reports</b></p> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div> <p><b>Firewall Log Management</b></p> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div> <p><b>Firewall Alerts</b></p> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div> <p><b>Firewall Compliance Management</b></p> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div> <p><b>Real-time Bandwidth Monitoring</b></p> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div> <p><b>Manage Firewall Service</b></p> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> </div> <p><a href="https://www.manageengine.com/products/firewall/firewall-rule-management.html">https://www.manageengine.com/products/firewall/firewall-rule-management.html</a></p>
code for displaying, via at least one user interface, a plurality of techniques of different technique types	ManageEngine includes a <i>code for displaying, via at least one user interface</i> (e.g., a user interface or web login on a computer used to monitor the devices on the Manage Engine platform), <i>a plurality of techniques of different technique types including a first technique for setting or modifying a policy for occurrence mitigation</i> (e.g., a policy for changing the patches or modifying or adding any policies in firewall or

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

including a first technique for setting or modifying a policy for occurrence mitigation, and a second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation;

vulnerability manager of the system), *and a second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation* (e.g., directly blocking or restricting the use of files or software that is found vulnerable to a threat);

**Note:** See, for example, the evidence below (emphasis added, if any):

### See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

### High Priority Vulnerabilities: Where your primary focus should be!

[Vulnerabilities](#) [Vulnerable Software](#)

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

Security Configuration Management with ManageEngine Vulnerability Manager Plus

ManageEngine Vulnerability Manager Plus

License Version : 10.0.621

HomeThreatsPatchesSystemsDeploymentReportsAgentAdminSupport

Threats

Software VulnerabilitiesZero-day VulnerabilitiesSystem MisconfigurationsHigh Risk SoftwareWeb Server MisconfigurationPort Audit

Update Vulnerability DB

Update Now

MORE VIDEOS

This view displays all the inappropriately configured security settings in your Windows systems.

Filter by:SeverityCategory

Misconfiguration

Geolocation is enabled to track location of users and devices

TLSv1.1 protocol is enabled

Administrative Shares enabled

Data Execution Prevention is not enabled

Maximum Password age is not configured to 45 days

Secure logon (Ctrl+Alt+Delete logon) is not enabled

Antivirus (not considering Windows Defender) not installed

Account lockout duration is not configured to 1440 minutes

Built-in Administrator Account is not disabled

Folder shares are assigned to everyone group

Windows firewall disabled/ No third-party firewall present

Outdated plugins are allowed to run

Category

Antivirus Protection

User Account Management

Windows Firewall

Password Policy

SSL and TLS Security

Chrome Security Hardening

Password Policy

Logon Security

Antivirus Protection

Logon Security

User Account Management

Share Permission Management

Windows Firewall

Chrome Security Hardening

Affected Systems

2

1

3

4

1

1

1

2

2

2

1

2

Severity

Info

Info

Info

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Total : 62

1 - 30 of 62

1:39 / 4:05 • Security Configuration Management

YouTube

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>



**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The left sidebar shows navigation options like Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is divided into several sections:

- Name and Description:** A text input field for 'Name' (currently 'No Configuration') and a link to 'Add Description'.
- Select Patch:** A section with 'Operation Type' (radio buttons for 'Install Patch' and 'Uninstall Patch'), a '+ Add Patches' link, and a table of available patches.
- Scheduler Settings (Optional):** Checkboxes for 'Install Only' and 'Do not apply Windows Configuration after the time specified below'.
- Deployment Rule:** A checkbox for 'Continue deployment even if some patches cannot be downloaded' with a note about failed patches.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' (set to 'Select Policy') and a link to 'Create Patch Policy'.
- Define Targets:** A section for 'Target 1' with a dropdown for 'Remote Office Domain' (set to 'Local Office') and a text input for 'Filter Computers based on' (set to 'Computer'). Below this is an 'Exclude Target' section with a dropdown for 'Domain' (set to 'Select').
- Execution Settings (Optional):** A section for 'Execution Settings'.

At the bottom left, there is a 'Update Vulnerability DB' button and a 'Last Update Time' of 'JUL 23 2024 10:03 AM'.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot displays the ManageEngine Vulnerability Assessment interface. The sidebar on the left contains navigation links such as 'System Health Summary', 'Highly Vulnerable Systems (3)', 'Vulnerable Systems (1)', 'Healthy Systems (6)', 'System Health Policy', 'Managed Systems', 'Scan Systems (13)', 'By Patches', 'By Vulnerabilities (7)', 'By Misconfigurations (8)', 'By Web Server Misconfiguration (5)', 'By High Risk Software (7)', 'Attention Required', 'Windows 10 EOL Systems', and 'Update Vulnerability DB'. The main content area is titled 'suraj-7073' and shows a 'Vulnerabilities' section. It includes a table with columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. The table lists three vulnerabilities, all with an exploit status of 'Not available' and a patch availability of 'Not available'. The CVSS 3.0 scores are 7.5, 7.5, and 6.9, while the CVSS 2.0 scores are 5.0, 5.0, and 7.5. The interface also includes filters for 'Severity' and 'Exploit Status', and a 'Total: 3' indicator.

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<p>code for receiving user input selecting the first technique for setting or modifying the policy for occurrence mitigation, utilizing the at least one user interface;</p> <p>code for, based on the user input selecting the first technique for setting or modifying the policy for occurrence mitigation, automatically applying the first technique for setting or modifying the policy for occurrence mitigation, such that an identification of a particular actual vulnerability to which the at least one networked device is actually vulnerable is used in connection with the first</p>	<p>ManageEngine includes a <i>code for receiving user input selecting the first technique for setting or modifying the policy for occurrence mitigation, utilizing the at least one user interface</i> (e.g., a user selecting the patches manually to stop or remove vulnerability by either of the ways, (i). clicking on the vulnerability and downloading the patch, (ii). Clicking on the patches and downloading or applying the remedies or, (iii). Searching the vulnerability by CEV ID of the vulnerability and then applying the patches for remedies of the vulnerability); <i>code for, based on the user input selecting the first technique for setting or modifying the policy for occurrence mitigation, automatically applying the first technique for setting or modifying the policy for occurrence mitigation, such that an identification of a particular actual vulnerability to which the at least one networked device is actually vulnerable is used in connection with the first technique, for mitigating a particular occurrence identified in connection with the at least one networked device if the at least one networked device is actually vulnerable to the particular actual vulnerability and the particular actual vulnerability is capable of being taken advantage of by the particular occurrence identified in connection with the at least one networked device, and further for not mitigating the particular occurrence if the particular actual vulnerability is incapable of being taken advantage of by the particular occurrence identified in connection with the at least one networked device;</i></p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>
--	---

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

technique, for mitigating a particular occurrence identified in connection with the at least one networked device if the at least one networked device is actually vulnerable to the particular actual vulnerability and the particular actual vulnerability is capable of being taken advantage of by the particular occurrence identified in connection with the at least one networked device, and further for not mitigating the particular occurrence if the particular actual vulnerability is incapable of being taken advantage of by the particular occurrence identified in connection with the at least one networked device;

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Home, Threats, Patches, Systems, Deployment, Reports, Agent, Admin, and Support. The main content area shows a list of misconfigurations. A filter dropdown is open, showing categories like Antivirus Protection, User Account Management, Windows Firewall, Password Policy, SSL and TLS Security, and Chrome Security Hardening. The 'Windows Firewall' category is highlighted with a red box. Below the filter, a table lists various misconfigurations. One row is highlighted with a red box, showing a critical issue: 'Windows firewall disabled/ No third-party firewall pre...' with a severity of 'Critical'.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	User Account Management	2	Info
TLSv1.1 protocol is enabled	Windows Firewall	1	Info
Administrative Shares enabled	Password Policy	3	Info
Data Execution Prevention is not enabled	Chrome Security Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

Security Configuration Management with ManageEngine Vulnerability Manager Plus

ManageEngine Vulnerability Manager Plus

License Version: 10.0.621

HomeThreatsPatchesSystemsDeploymentReportsAgentAdminSupport

Threats

Software Vulnerabilities

Zero-day Vulnerabilities

System Misconfigurations

High Risk Software

Web Server Misconfiguration

Port Audit

This view displays all the inappropriately configured security settings in your Windows systems.

Filter by:SeverityCategory

Misconfiguration

Geolocation is enabled to track users' physical location

TLSv1.1 protocol is enabled

Administrative Shares enabled

Data Execution Prevention is not enabled

Maximum Password age is not configured to 42 days

Secure logon (Ctrl+Alt+Delete logon) is not enabled

Antivirus (not considering Windows Defender) is not installed

Account lockout duration is not configured to 30 minutes

Built-in Administrator Account is not disabled

Folder shares are assigned to everyone group

Windows firewall disabled/ No third-party firewall present

Outdated plugins are allowed to run

Update Vulnerability DB

Update Now

Last Update Time: Oct 5, 2020 07:49 PM

Misconfiguration Details

Name

Description

Severity

Misconfigured in Domain GPO

Solution

Resolution

Post Deployment Issues

: Data Execution Prevention is not enabled

: DEP/NX (Data Execution Prevention/ No Execution) marks the memory pages as executable and non-executable. Further, it detects the presence of executable data in non-executable memory page and terminates the execution of malicious code placed by an attacker. DEP is a highly effective security feature that must be enabled in your network computers.

: Critical

: No

Deploy Secure Configuration

: Some legacy applications are not compatible with DEP (Data Execution Prevention) and might crash when DEP is enabled. You can exclude such applications from DEP settings. Also, the potential impact varies depending on the importance of applications and services that are dependent on DEP (attach an error kb on how to exclude applications from DEP settings)

Severity

Info

Info

Info

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Critical

Total: 62

1 - 30 of 62

1:11 / 4:05 • Security Configuration Management >

Scroll for details

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

41

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

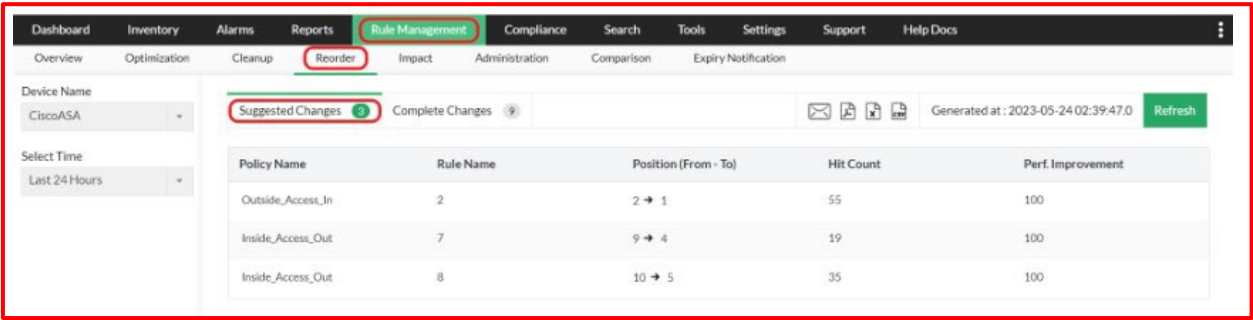
Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**3. Firewall Rule Reorder Recommendations**



Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Other features****Firewall Reports**

Get a slew of security and traffic reports to assess the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.

**Firewall Log Management**

Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.

**Firewall Alerts**

Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.

**Firewall Compliance Management**

Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.

**Real-time Bandwidth Monitoring**

With live bandwidth monitoring, you can identify the abnormal sudden shoot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.

**Manage Firewall Service**

MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the ManageEngine Vulnerability Management console. The left sidebar contains navigation options: Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is titled 'Install/Uninstall Windows Patch (Computer)' and includes sections for Name and Description, Install Patch, Scheduler Settings (optional), Deployment Rule, Deployment Settings, Define Targets, and Execution Settings (optional). The 'Define Targets' section shows a table with columns for Patch ID, Patch Description, Patch Type, Patch Type, Approval Status, Missing Systems, Installed Systems, and Action. The table lists two patches: 'Security Update for Windows 8.1 KB3033920' and 'Security Update for Windows 8.1 KB3033920'. The 'Deployment Settings' section includes a dropdown for 'Apply Deployment Policy' and a 'Create Policy' button. The 'Define Targets' section includes a 'Target 1' dropdown and a 'Filter Computers based on' dropdown.

Patch ID	Patch Description	Patch Type	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
KB3033920	Security Update for Windows 8.1 KB3033920	Windows Update	Security Update	Approved	1	0	Re
KB3033920	Security Update for Windows 8.1 KB3033920	Windows Update	Security Update	Approved	1	0	Re

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot shows the ManageEngine Vulnerability Assessment interface. The left sidebar contains navigation options like 'System Health Summary', 'Highly Vulnerable Systems', 'Vulnerable Systems', 'Healthy Systems', 'System Health Policy', 'Managed Systems', 'Scan Systems', 'By Patches', 'By Vulnerabilities', 'By Misconfigurations', 'By Web Server Misconfiguration', 'By High Risk Software', 'Attention Required', and 'Windows 10 EOL Systems'. The main content area is titled 'suraj-7073' and shows the 'Vulnerabilities' section. The 'Web' tab is selected, displaying a table of vulnerabilities. The table has columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. There are three vulnerabilities listed, all with an exploit status of 'Not available' and a patch availability of 'Not available'.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527/CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329/CVE-2020-9484/CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

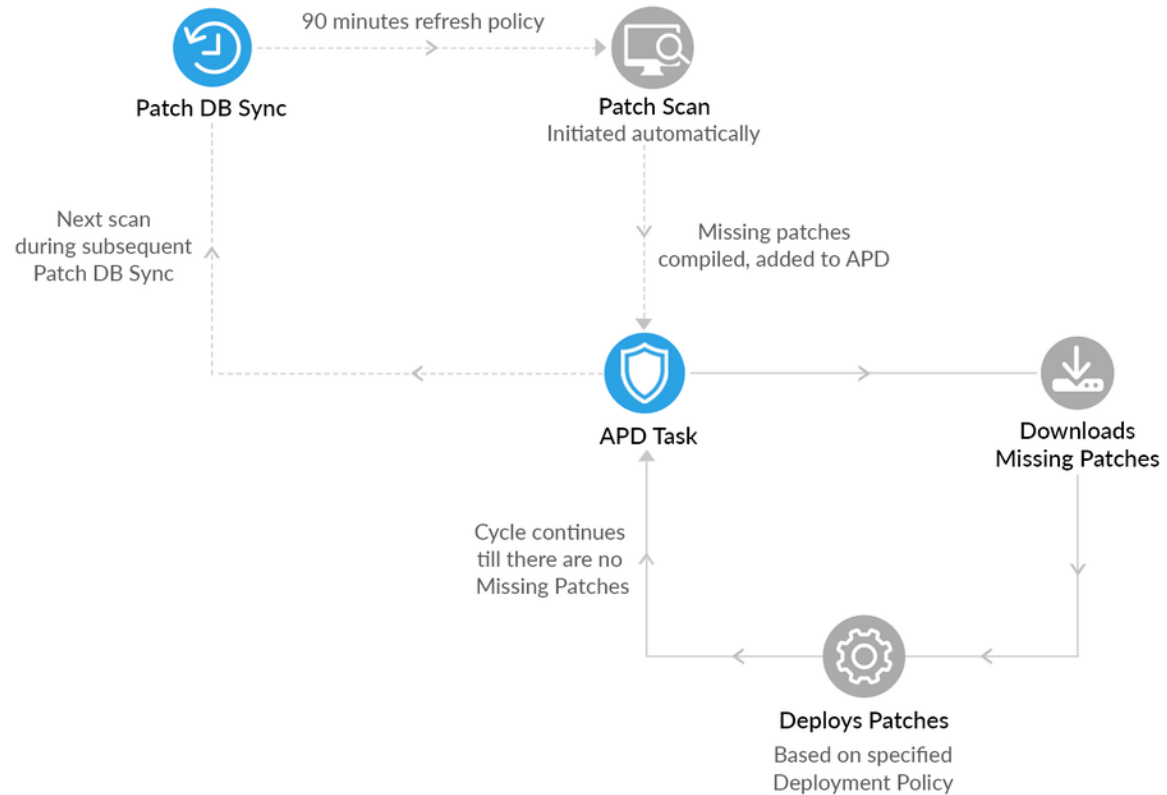
- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Automate Patch Deployment Task Workflow**



<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**| Need for Automated Patch Deployment:**

With the steady rise in attack vendors and frequency of attacks, it is mandatory to keep all your enterprise endpoints up to date and round the clock patched. The best way to address this problem, is to have a systematic and automated solution that manages multiple OSs and third party application patches effectively.

The **Automate Patch Deployment** (APD) feature provides system administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention required.

**| Automate Patch Deployment (APD) workflow has been enhanced!**

To keep up with cyber industry's security demands and requests from a few customers, ManageEngine's **Patch Management** module has undergone a few enhancements in the '**Automated Patch Deployment**' (APD) functionality. We will shed light on what's new with the latest APD feature.

<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Benefits of new-feel Automated Patch Deployment</b></p> <ol style="list-style-type: none"> <li>1. Deployments are fast, and security is tightened due to the readily available patches for deployment.</li> <li>2. All the approved patches will be deployed in the very next deployment window immediately after their download. There's no need to wait for the next APD scheduler to invoke the deployment.</li> <li>3. Whenever the computer in the network goes offline and encounters the network connectivity again, there could be new vulnerabilities and patches that the computer be missing. In the new APD, when the agent comes into contact with the server, it gets automatically scanned in the next refresh cycle, the missing patches are detected and updated in the server. The agent deploys them in the subsequent refresh cycle during the deployment window. Hence, there is no need to worry about the agent contact time and its prolonged vulnerable status. In the old APD, patch installation might be delayed because the agent contacted the server only after APD schedule.</li> <li>4. Deployment in agent continues until it gets zero missing patches for the APD criteria.</li> <li>5. In the new APD, you can also see the history of patching in a more detailed view.</li> </ol> <p><a href="https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html">https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html</a></p>
code for receiving user input selecting the second technique for reacting to packets in connection with the at least one networked device for occurrence	<p>ManageEngine includes a <i>code for receiving user input selecting the second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation, utilizing the at least one user interface; and</i> (e.g., a user selecting the patches automatically via Automated Patch Deployment based on the identified vulnerability wherein the automated vulnerabilities can be downloaded by the system based on the global threat standards or can be selected by a user for automatic deployment with user defined parameters and techniques performed every time a vulnerability is detected), <i>code for, based on the</i></p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

mitigation, utilizing the at least one user interface; and

code for, based on the user input selecting the second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation, automatically applying the second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation, such that an identification of a certain actual vulnerability to which the at least one networked device is actually vulnerable is used in connection with the second technique, for reacting to packets in

*user input selecting the second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation, automatically applying the second technique for reacting to packets in connection with the at least one networked device for occurrence mitigation, such that an identification of a certain actual vulnerability to which the at least one networked device is actually vulnerable is used in connection with the second technique, for reacting to packets in connection with a certain occurrence identified in connection with the at least one networked device if the at least one networked device is actually vulnerable to the certain actual vulnerability and the certain actual vulnerability is capable of being taken advantage of by the certain occurrence identified in connection with the at least one networked device, and further for not reacting, at least in part, to packets in connection with the certain occurrence if the certain actual vulnerability is incapable of being taken advantage of by the certain occurrence identified in connection with the at least one networked device;*

**Note:** See, for example, the evidence below (emphasis added, if any):

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

connection with a certain occurrence identified in connection with the at least one networked device if the at least one networked device is actually vulnerable to the certain actual vulnerability and the certain actual vulnerability is capable of being taken advantage of by the certain occurrence identified in connection with the at least one networked device, and further for not reacting, at least in part, to packets in connection with the certain occurrence if the certain actual vulnerability is incapable of being taken advantage of by the certain occurrence identified in

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Home, Threats, Patches, Systems, Deployment, Reports, Agent, Admin, and Support. The main content area is titled 'This view displays all the inappropriately configured security settings in your Windows systems.' It features a table of misconfigurations with columns for Category, Affected Systems, and Severity. A filter dropdown is open, showing 'Windows Firewall' selected. The table lists various security settings, with the entry 'Windows firewall disabled/ No third-party firewall pre...' highlighted in red, indicating a 'Critical' severity.

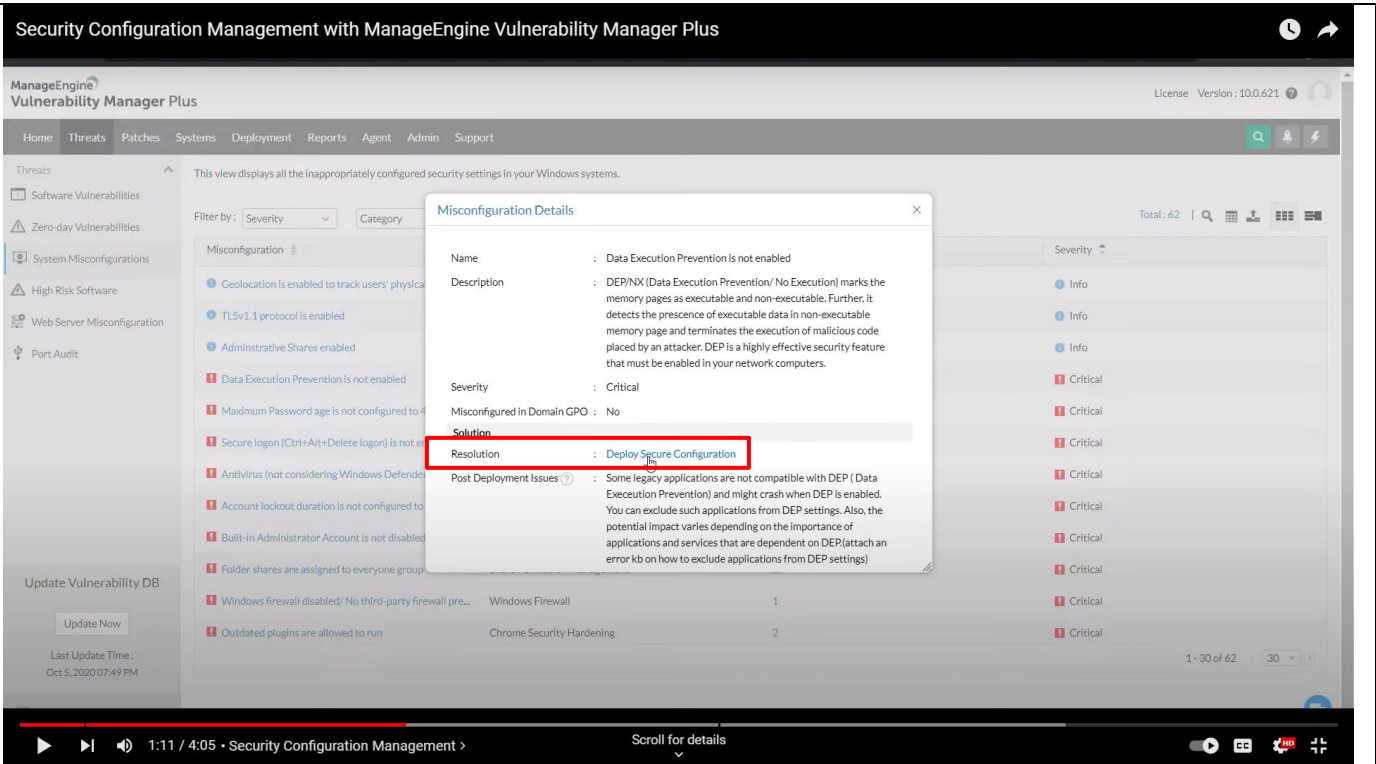
Category	Affected Systems	Severity
Geolocation is enabled to track	2	Info
TLSv1.1 protocol is enabled	1	Info
Administrative Shares enabled	3	Info
Data Execution Prevention is r	4	Critical
Maximum Password age is not configured to 45 days	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	1	Critical
Antivirus (not considering Windows Defender) not inst...	1	Critical
Account lockout duration is not configured to 1440 mi...	2	Critical
Built-in Administrator Account is not disabled	2	Critical
Folder shares are assigned to everyone group	2	Critical
Windows firewall disabled/ No third-party firewall pre...	1	Critical
Outdated plugins are allowed to run	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

connection with the at least one networked device;



<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the ManageEngine Vulnerability Management console. The left sidebar contains navigation options: Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is titled 'Install/Uninstall Windows Patch (Computer)' and includes sections for 'Name and Description', 'Install Patch', 'Schedule Settings (Optional)', 'Deployment Rule', 'Deployment Settings', 'Define Target', and 'Execution Settings (Optional)'. The 'Install Patch' section features a table of patches with columns for Patch ID, Patch Description, Patch Type, Patch Name, Approval Status, Missing Systems, Installed Systems, and Action. Two patches are listed: 'Security Update for Windows 8.1 KB3033950' and 'Security Update for Windows 8.1 KB3033950'. The 'Define Target' section shows a list of targets, including 'Remote Office Domain' and 'Local Office', with a filter for 'Computer' and a search bar.

Patch ID	Patch Description	Patch Type	Patch Name	Approval Status	Missing Systems	Installed Systems	Action
16340	Security Update for Windows 8.1 KB3033950	Hotfix	Security Update	Approved	1	0	Re
16340	Security Update for Windows 8.1 KB3033950	Hotfix	Security Update	Approved	1	0	Re

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot shows the ManageEngine Vulnerability Assessment interface. The left sidebar contains navigation options like System Health Summary, Highly Vulnerable Systems, Vulnerable Systems, Healthy Systems, System Health Policy, Managed Systems, Scan Systems, By Patches, By Vulnerabilities, By Misconfigurations, By Web Server Misconfiguration, By High Risk Software, Attention Required, and Windows 10 EOL Systems. The main content area is titled 'suraj-7073' and shows the 'Vulnerabilities' section. The 'Web' tab is selected, displaying a table of vulnerabilities. The table has columns for Vulnerabilities, File Path, Exploit Status, Patch Availability, CVSS 3.0 Score, and CVSS 2.0 Score. Three vulnerabilities are listed, all with an exploit status of 'Not available' and a patch availability of 'Not available'.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527/CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329/CVE-2020-9484/CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

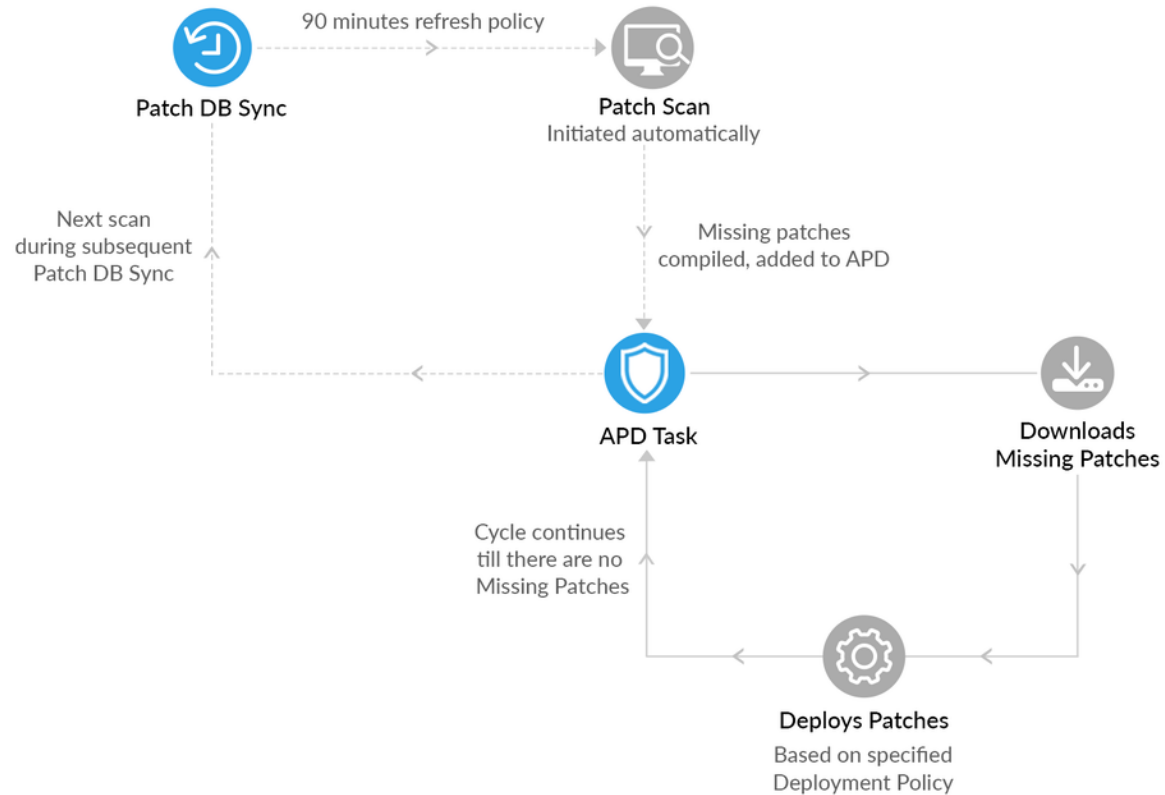
- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Automate Patch Deployment Task Workflow**



<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<p>  Need for Automated Patch Deployment:</p> <p>With the steady rise in attack vendors and frequency of attacks, it is mandatory to keep all your enterprise endpoints up to date and round the clock patched. The best way to address this problem, is to have a systematic and automated solution that manages multiple OSs and third party application patches effectively.</p> <p>The <b>Automate Patch Deployment</b> (APD) feature provides system administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention required.</p> <p>  Automate Patch Deployment (APD) workflow has been enhanced!</p> <p>To keep up with cyber industry's security demands and requests from a few customers, ManageEngine's <b>Patch Management</b> module has undergone a few enhancements in the '<b>Automated Patch Deployment</b>'(APD) functionality. We will shed light on what's new with the latest APD feature.</p> <p><a href="https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html">https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html</a></p>
--	--

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Benefits of new-feel Automated Patch Deployment</b></p> <ol style="list-style-type: none"> <li>1. Deployments are fast, and security is tightened due to the readily available patches for deployment.</li> <li>2. All the approved patches will be deployed in the very next deployment window immediately after their download. There's no need to wait for the next APD scheduler to invoke the deployment.</li> <li>3. Whenever the computer in the network goes offline and encounters the network connectivity again, there could be new vulnerabilities and patches that the computer be missing. In the new APD, when the agent comes into contact with the server, it gets automatically scanned in the next refresh cycle, the missing patches are detected and updated in the server. The agent deploys them in the subsequent refresh cycle during the deployment window. Hence, there is no need to worry about the agent contact time and its prolonged vulnerable status. In the old APD, patch installation might be delayed because the agent contacted the server only after APD schedule.</li> <li>4. Deployment in agent continues until it gets zero missing patches for the APD criteria.</li> <li>5. In the new APD, you can also see the history of patching in a more detailed view.</li> </ol> <p><a href="https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html">https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html</a></p>
<p>wherein the computer program product is operable such that at least one of:</p> <p>said at least one first data storage includes at least one first database; said at least</p>	<p>ManageEngine includes <i>a computer program product is operable such that at least one of: said at least one first data storage includes at least one first database; said at least one first data storage is a component of a network operations center (NOC) server (e.g., the Central Vulnerability Database situated on the server side of the architecture for storing global vulnerabilities and keeping them available for network devices); said at least one second data storage includes at least one second database (e.g., network devices or endpoints having storage to store device-specific data);</i></p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

one first data storage is a component of a network operations center (NOC) server;

said at least one second data storage includes at least one second database;

**Note:** See, for example, the evidence below (emphasis added, if any):

### **Comprehensive vulnerability scanning**


Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.


<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The top navigation bar includes links for Dashboard, Threats, Patches, Deployment, Systems, Reports, Agent, Admin, and Support. The left sidebar lists various threat categories: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' It features a search bar and a table of vulnerabilities.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

At the bottom right of the table, it shows '1 - 5 of 5' and a dropdown menu set to '30'.

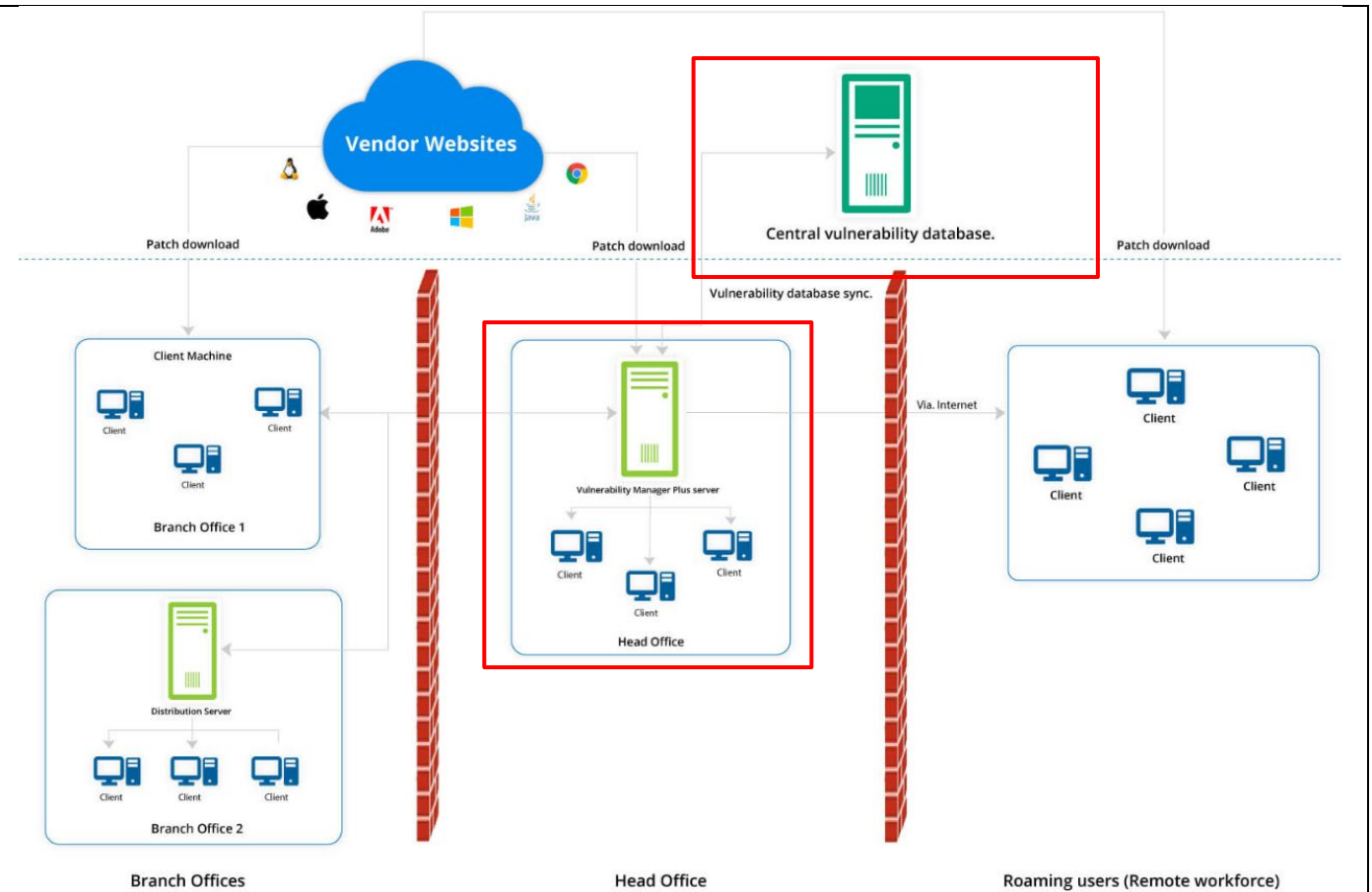
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****See what matters most at a glimpse with dashboard widgets**

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

**High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<p>said allowed access to the first information from the at least one first data storage is accomplished by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;</p>	<p>ManageEngine discloses that <i>said allowed access to the first information from the at least one first data storage is accomplished by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith</i> (e.g., the patches serving as remedies for the vulnerabilities are stored in the Central Vulnerability Database wherein the patches when set to automatic deployment are downloaded from the database and installed on the system. Further, when the vulnerability is evolving with time the patches also need to be updated with time and hence are synchronized with the database to receive timely updates);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>
---	--

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**| How to automate your organization's patch management schedule?**

It's safe to assume that vulnerabilities are a constant threat to the network. Manual intervention is required to accurately assess and address the high profile vulnerabilities consistently. But given the rate at which new vulnerabilities surface, manually it's both easy to overlook certain critical vulnerabilities, as well difficult to reduce the total number of unpatched vulnerabilities in your network.

While you focus on what matters the most, let Vulnerability Manager Plus' built-in patching module regularly clean up the vulnerabilities in your network by automating the entire cycle of patching—including missing patch detection, download, testing, and deployment—to Windows, Mac, Linux, and over 300 third-party applications. The comprehensive patching functionality enables you to choose the criteria of patches to be automated, specific target machines/custom groups to be patched, flexible deployment policies, patch testing, and approval as well as deployment schedules based on your business requirements. What's more, you can use pre-built Patch Tuesday-based deployment policies to synchronize your patching with monthly Patch Tuesdays, and more. Explore the exhaustive capabilities of Vulnerability Manager Plus' [automated patch management](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html?meseach>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**| Automated patch deployment:**

Achieve cradle to grave automation in patching right from detecting missing patches in all the endpoints, downloading them respective vendors, testing them out for stability till deploying them to production machines.

- Keep abreast of frequent release of patches from multiple vendors.
- Schedule scans by time, computer, group or user-defined collections of computers and continuously monitor missing patches on the endpoints.
- Select the criteria of patches you wish to deploy and select target machines/ groups for your deployment, and let patch management takes care of everything else.
- Gain Periodic updates on patch deployment status and redeploy failed patches without having to lift a finger.

**| Deployment policies:**

Customize your patch management process on when and how patches should be deployed to users' machines, and what should happen after patch deployment.

- Configure preferred weeks, days and window for deployment based on your needs.
- Initiate deployment either during system start-up or refresh, or whichever is earlier.
- Wake shut down computers before deployment using Wake-ON LAN feature.
- Download patches on the client machine during subsequent refreshes, even before the deployment window.
- Notify users on deployment, allow them to postpone deployment or force deployment on their machines.
- Carefully craft shutdown, reboot policies for critical machines like web servers, database servers, etc.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/patch-management.html>

## Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the ManageEngine Vulnerability Management console. The left sidebar contains navigation options: Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is titled 'Install/Uninstall Windows Patch (Computer)' and includes sections for Name and Description, Install Patch, Operation Type (Install Patch selected), a table of patches, Scheduler Settings, Deployment Rule, Deployment Settings, Define Targets, and Execution Settings.

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16340	Security Update for Windows 8 KB3033920	May Require	Security Updates	Approved	1	0	R
27504	Security Update for Windows 8 KB3033920	May Require	Security Updates	Approved	1	0	R

Below the table, the 'Define Targets' section shows a list of targets with columns for Name, Remote Office Domain, and Local Office. The 'Local Office' column is currently empty.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot displays the ManageEngine Vulnerability Assessment interface. The sidebar on the left contains navigation links such as 'System Health Summary', 'Highly Vulnerable Systems (3)', 'Vulnerable Systems (1)', 'Healthy Systems (6)', 'System Health Policy', 'Managed Systems', 'Scan Systems (13)', 'By Patches', 'By Vulnerabilities (7)', 'By Misconfigurations (8)', 'By Web Server Misconfiguration (5)', 'By High Risk Software (7)', 'Attention Required', and 'Windows 10 EOL Systems'. The main content area is titled 'suraj-7073' and shows a 'Vulnerabilities' section. The 'Web' tab is selected, displaying a table of vulnerabilities. The table has columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. Three vulnerabilities are listed, all with an exploit status of 'Not available' and a patch availability of 'Not available'.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527/CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329/CVE-2020-9484/CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<p>said potential vulnerabilities and the actual vulnerabilities include software vulnerabilities in an application or an operating system that are capable of being exploited by an attack or a virus;</p> <p>said at least one operation includes a vulnerability scan operation;</p>	<p>ManageEngine discloses that <i>said potential vulnerabilities and the actual vulnerabilities include software vulnerabilities in an application or an operating system</i> (e.g., vulnerabilities on the network devices include software-based vulnerabilities like end-of-life software, virus attacks, malware attacks, remote desktop sharing, etc. that are operated on the operating system of the devices including updates of the operating system) <i>that are capable of being exploited by an attack or a virus; said at least one operation includes a vulnerability scan operation</i> (e.g, a virus attack on the network devices which is avoided by performing a virus scan on the device using firewall analyzer which will identify and provide remedies for the virus attack to be suppressed);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p> <p style="text-align: center;"><b>High risk software audit</b></p> <div style="border: 1px solid red; padding: 10px; margin: 10px 0;"> <p>The proliferation of devices and software has inevitably caused enterprises to serve as a home for a number of unsupported and unauthorized software. These software might bring a lot of security risks such as information disclosure, malicious code injection, unauthorized access that damages the organization's security and reputation. Take a brief look at the impacts of such software to your network.</p> </div>
---	--

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<p data-bbox="632 254 1138 293"><b>Dangers of high-risk software</b></p> <hr data-bbox="632 321 1633 328"/> <p data-bbox="632 354 915 393">  End of life software</p> <div data-bbox="617 427 1892 651" style="border: 2px solid red; padding: 10px;"><p data-bbox="632 435 1877 638">End of life software are rampant in enterprises due to lack of visibility and poor management. The consequences of running an end of life software outweighs its benefits. End of life OS and applications will not receive security updates from vendors to patch critical vulnerabilities, which makes them extremely vulnerable to exploits. Moreover, Legacy OSes can't run latest applications and they'll be stuck with legacy applications which will soon become end of life too, thus widening the attack surface. Also, businesses in regulated industries may also face significant fines for running out-of-date systems.</p></div> <p data-bbox="575 695 1715 730"><a href="https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html">https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html</a></p>
--	---

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<p><b>  Peer to peer software</b></p> <p>P2P(Peer to Peer) applications such as Overnet, Morpheus, SoMud, GigaTribe allows a user to share and receive files over the internet. Files shared through Peer to Peer applications may be a pirated software, or copyrighted material which might land you in trouble for being involved in illegal actions. Also, the reliability of files shared through peer to peer software can't be verified which gives an attacker a leeway to transmit malicious code along with the file you download. Users might be unaware of what folders they are sharing which might allow unauthorized access to sensitive information stored in their computers. Some peer to peer applications may ask you to open certain ports on your firewall to transmit the files. This might allow an attacker to exploit the loopholes associated with the port or take advantage of any vulnerabilities that may exist in the peer to peer application.</p> <p><b>  Remote Desktop Sharing Software:</b></p> <p>IT employees often use remote desktop sharing software to facilitate remote access and management of remote server, virtual desktops, terminal servers, and applications over internet for the ease of operation. It's true that a remote desktop sharing software improves productivity, but it also increases the attack surface leaving an attacker to gain control over business critical assets once he finds a way to exploit the computer which is used to access them remotely. Also, if the remote desktop sharing sessions are not encrypted, it might increase the possibility of a Man-in-the-middle (MitM) attack.</p> <p><a href="https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html">https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html</a></p>
--	--

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Audit and eliminate high-risk software in your network</b></p> <hr/> <p>The above cited reasons explains the importance of auditing such high risk software that may be installed in network systems without the administrator's knowledge. With Vulnerability Manager Plus at your disposal, you can</p> <ul style="list-style-type: none"><li>• Monitor your network endpoints continuously and detect end of life softwares, peer to peer softwares and remote sharing tools present in them.</li><li>• Get details on the expiry date and the number of days before software in your network becomes end of life.</li><li>• Obtain real-time information on the number of machines that are affected by these software.</li><li>• Eliminate these software with just a click of a button from the console.</li></ul> <p><a href="https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html">https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html</a></p>
--	---

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**How Vulnerability Manager Plus helps you fortify your network against zero-days and public disclosures?**

- Vulnerability Manager Plus includes a dedicated tab that displays zero-day and publicly disclosed vulnerabilities separately from other exploits so that you can instantly identify and respond to them.
- Generally, it takes two or more vulnerabilities to successfully launch a zero-day attack. With automated patching, you can stay current with the latest updates for all your OS and applications, thereby hampering the attacker's attempts.
- Vendors generally quickly publish work-arounds for public disclosures while they work on a fix. You can deploy these work-arounds to all the affected machines in an instant with Vulnerability Manager Plus' pre-built mitigation scripts.
- As long as your antivirus protection is up-to-date, you should be protected within a short time of a new zero-day threat. The antivirus audit feature enables you to sniff out endpoints with missing, disabled, or out-of-date antivirus programs. If your systems are running an outdated antivirus application, you can leverage Vulnerability Manager Plus' patch management feature to keep your antivirus up-to-date with the latest definition files.
- Your best bet against a zero-day threat is to harden the security of your IT ecosystem. Utilize the security configuration management feature to block vulnerable ports, disable legacy protocols, close insecure firewall connections, and disable unintended network shares with excessive permissions that usually serve as the vectors for malware to progress through the network laterally.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html?meseach>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

ManageEngine Rounds off Its Endpoint Protection Platform with the Addition of Next Generation Antivirus Capability

Capability Added to Endpoint Central, its UEM Solution, to Tackle the Dynamic Threat Landscape

- Proactive, AI-based protection with real-time monitoring for known and unknown threats
- Unified approach promotes interoperability between IT functions, simplifying threat detection, investigation and remediation
- Download a 30-day, free trial of Endpoint Central at <https://mnge.it/NGAV>

Benefits of Endpoint Central's NGAV

Endpoint Central uses a single, lightweight agent for its wide range of high-stakes capabilities like device life cycle management, remote troubleshooting, user experience management and endpoint security.

Apart from reducing organizations' IT footprints, this unified approach offers:

- **A wide scope for remediation policies:** Security teams can apply necessary patches, quarantine affected devices from the internet and intranet, force login credential resets, revert devices to their IT-approved baseline versions and remove vulnerable applications.
- **Seamless incident investigation:** Built-in remote troubleshooting and system management capabilities offer instant and thorough incident investigation of quarantined devices.
- **Feedback loops for bolstering the security posture:** Security policies can be continuously updated based on threats detected by the NGAV engine, constantly enhancing the cybersecurity posture.

ManageEngine has been in the IT management market for over 20 years and has built a strong foundation of IT management and security capabilities from the ground up. The NGAV addition to Endpoint Central is a move to strengthen endpoint security within the company's comprehensive portfolio of cybersecurity solutions.

"We aim to offer an AI-powered, unified, end-to-end platform for the digital enterprise in which cyber resilience is of paramount importance," added Venkatachalam. "The platform will enable customers to devise and implement a comprehensive security strategy by building workflows across multiple ManageEngine security offerings, automating threat detection, threat responses and incident investigation."

<https://www.manageengine.com/news/manageengine-rounds-endpoint-protection-platform-addition-next-generation-antivirus-capability.html?meseach>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<div data-bbox="617 264 1570 305"><b>Virus, Attack, Security, and Spam Reports from Firewall Logs</b></div> <div data-bbox="617 342 1310 378"><b>Detailed Security, Virus, Attack and Spam Analysis</b></div> <div data-bbox="617 415 1871 513"><p>Firewall Analyzer includes instant reports on <a href="#">viruses</a>, <a href="#">attacks</a> and <a href="#">security</a> breach in your network. These reports instantly show you the <a href="#">viruses active</a> on the network, the hosts that have been affected, and more. With these reports it is easier for IT to do business risk assessment, detect problems and resolve them as soon as they are found.</p></div> <div data-bbox="625 578 827 613"><b>Virus Reports</b></div> <div data-bbox="625 652 1879 756"><p><a href="#">Virus reports</a> give in-depth information on virus attacks, <a href="#">hosts infected</a>, severity of the attack, subtype, and more. With drillable details to the raw log level on <a href="#">top viruses</a> and top protocols used by viruses, the complete details of the virus related raw log is available. The raw log message make troubleshooting and problem resolution faster and more efficient.</p></div> <div data-bbox="573 803 1549 839"><p><a href="https://www.manageengine.com/products/firewall/firewall-virus-report.html">https://www.manageengine.com/products/firewall/firewall-virus-report.html</a></p></div>
--	--

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

Custom Report

Firewall Reports

Proxy Reports

API Access

General

Device Name

All Devices

Report Type

Security Reports

Virus Reports

Attack Reports

Spam Reports

Protocol Trend Reports

Traffic Trend Reports

Event Trend Reports

Admin Reports

VPN Trend Report

URL Report

Active VPN Trend

Virus Reports

Today

Top Virus Sending Hosts

Resolve DNS

Host	smtp	http	ftp
64.41.199.20	42	0	0
192.168.4.74	15	0	0
192.168.4.32	0	80	0
192.168.4.136	0	15	0
192.168.4.143	0	0	28

Host

Protocol

Hits

192.168.4.32

http

80

Top Virus Affected Hosts

Resolve DNS

Destination	smtp	http	ftp
192.168.4.74	42	0	0
216.104.212.81	0	8	0
208.50.102.119	0	8	0
66.35.199.25	0	0	25
64.41.199.25	0	0	8

Destination

Protocol

Hits

192.168.4.74

smtp

42

<https://www.manageengine.com/products/firewall/firewall-virus-report.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<h2>Antivirus audit made easy!</h2> <p>Malware and viruses can penetrate your network in thousands of ways. Modern-day attacks involve sophisticated malware that can easily circumvent carefully crafted firewall rules and other security-hardening measures. Therefore, it's necessary to have standard antivirus software installed in your network devices to catch these malware as they appear. On an enterprise level, auditing the antivirus protection would become challenging due to a significant number of endpoints in the network and the constant addition of new endpoints to the existing horde.</p> <p>Here is where Vulnerability Manager Plus' comes into play. With Vulnerability Manager Plus' antivirus audit, you can automatically scan your endpoints for antivirus presence and identify the installed antivirus software in your devices from a centralized console. New viruses are detected every day by antivirus software. And vendors are coming up with definition updates to address them. Hence, antivirus software requires to be up-to-date with the latest antivirus definitions.</p> <p>Vulnerability manager plus helps you to identify systems in which the installed antivirus is disabled and not up-to-date with the latest antivirus definitions. With this information, you can detect security weaknesses in your network and rectify them to improve your security posture against malware and viruses.</p> <p><a href="https://www.manageengine.com/vulnerability-management/antivirus-audit.html">https://www.manageengine.com/vulnerability-management/antivirus-audit.html</a></p>
<p>said at least one configuration includes at least one of service pack information, elements contained in files including at least one of an *.ini or *.conf file, an aspect</p>	<p>ManageEngine discloses that <i>said at least one configuration includes at least one of service pack information, elements contained in files including at least one of an *.ini or *.conf file, an aspect of an operating system, or registry information</i> (e.g., the Security Configuration Management will check for any misconfiguration across various components of the network devices wherein the configuration details are extracted by auditing the .conf or .ini files of the software including the updates or any password or security compromise in the device or its operating system);</p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

of an operating system, or registry information;

**Note:** See, for example, the evidence below (emphasis added, if any):

## Security Configuration Management (SCM) : Establish a secure foundation

Time to time, zero-days will rear their ugly heads, so poise yourself with a secure foundation by ensuring ideal security configurations are established and maintained in your endpoints, so that your organization doesn't fall apart from a single vulnerability.

Security configuration management involves continually detecting configuration drifts and misconfigurations across various components in your endpoints, and bringing them back into alignment.

In this article, you'll learn how Vulnerability Manager Plus, a complete threat and [vulnerability management solution](#), facilitates the entire cycle of security configuration management including detecting misconfigurations, categorizing and profiling them, resolving them with built-in remediation, and reporting the final configuration posture—all from a single interface.

Equip yourself with the Vulnerability Manager Plus's Security Configuration Management dashboard, built exclusively to track and combat misconfigurations - [try now for free!](#)

<https://www.manageengine.com/vulnerability-management/security-configuration-management.html>

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

ManageEngine

Vulnerability Manager Plus

License Build Version:10.0.333

Dashboard

Threats

Patches

Deployment

Systems

Reports

Agent

Admin

Support

Vulnerabilities

Security Configurations

Systems

Patches

39

Total System Misconfigurations

36

Fixable System Misconfigurations

6

Misconfigured in Domain GPO

19

Web Server Misconfiguration

System Misconfigurations

Misconfiguration	Affected Systems	Category
Administrative Shares enabled	1	Share Permission Management
Secure password length is not configured (must be set to 15 characters)	2	Password Policy
Maximum Password age is not configured to 45 days	2	Password Policy
BitLocker not enabled	1	BitLocker Encryption
Account lockout duration is not configured to 1440 mins (1 day)	2	Logon Security
Administrator accounts are enumerated during elevation	1	Logon Security
User rights granted to everyone group	1	Account Privilege Management
"Always install with elevated privileges" is not disabled	1	Account Privilege Management
User Account Control (UAC) is not configured to "always notify"	2	Account Privilege Management
"Disallow Autoplay for non-volume devices" is not enabled	1	OS Security Hardening

View More

BitLocker Disabled Systems

1

Firewall Disabled Systems

2

SSL Expired Servers

1

Windows Defender Disabled Systems

1

<https://www.manageengine.com/vulnerability-management/security-configuration-management.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

| Firewall audit.

A firewall misconfiguration can fail to prevent unsecure traffic from penetrating an endpoint in your network. With security configuration management, you can check whether a built-in windows firewall is enabled or a third-party firewall is present.

You can also ensure connections are blocked in the firewall to the NetBIOS trio, the infamous WannaCry abettor port 445, and other vulnerable ports that allow unauthorized and unintended actions.

| Password policies.

Weak passwords are the most common security misconfiguration that plagues the enterprises quite often. "The longer the password, the stronger it is" no longer applies. Attackers are constantly developing new strategies, such as purchasing credentials used in previous breaches to launch password-based brute force and dictionary attacks. Moreover, 62 percent

of users admit reusing a password. Besides enforcing long passwords, you can make users adhere to a mix of predefined password policies such as password complexity, minimum password age, maximum password age, how many unique passwords that must be used before old passwords can be reused.

<https://www.manageengine.com/vulnerability-management/security-configuration-management.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Measure, Track, analyse your progress with insightful reports:

Your entire [vulnerability management](#) program becomes futile if you can't evaluate your efforts and understand your security stance. Vulnerability manager Plus brings you massive collection of pre-defined, insightful reports that you can use to scrutinize your network security, communicate risks, track progress and report on security regulations to executives.

These reports comes in different formats to cater to your needs. You can also schedule reports to security executives, administrators and enterprise risk management teams with just a click from the console.

### Executive asset summary:

Get an overview of the assets you manage and insights on critical assets that should be prioritized.

### Executive vulnerability summary:

The executive vulnerability summay report helps you gain detailed information on vulnerabilities, security misconfigurations, high risk softwares, vulnerable ports and webserver flaws in your network.

### Executive patch summary:

Executive patch summary report provides an overview of missing patches and deployments that help you track the measures taken to safeguard your enterprise.

### Threat priority report:

The threat priority report gives you a prioritized list of the assets, vulnerabilities, misconfigurations and other threats that are more likely to be exploited and needs immediate attention.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/insightful-reports.html>

| Pre-defined reports - Dig a level deeper into your security exposure.

Patch reports:

**Vulnerable patches:**

This report displays a list of all the missing patches in the network and details on affected systems for every patch that is listed.

**Supported patches:**

This report delivers details on all the patches released by Microsoft Corporation irrespective of whether these patches have a relation to your network or not. This report will be of absolute use when you plan to upgrade the systems in your network by installing the latest applications/ updates available for the application.

**Missing patches awaiting approval:**

This report will list down all the tested patches that are missing in your endpoints but have not been approved for deployment.

**Remote office patch summary:**

The Remote Office Patch Summary Report lists down the number of missing patches, installed patches, applicable patches, healthy systems, vulnerable systems, highly vulnerable systems and managed computers by your remote offices.

<https://www.manageengine.com/vulnerability-management/insightful-reports.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<p>said determination that the at least one networked device is actually vulnerable to the one or more actual vulnerabilities, is carried out by utilizing at least one of a vulnerability identifier or a profile;</p>	<p>ManageEngine discloses that <i>said determination that the at least one networked device is actually vulnerable to the one or more actual vulnerabilities, is carried out by utilizing at least one of a vulnerability identifier or a profile</i> (e.g., the vulnerabilities identified by the Vulnerability Manager Plus will be stored in the Central Vulnerability Database wherein the database also provides every vulnerability with a CVE ID which is unique to every vulnerability so that in case a user want to access and apply patches for a specific vulnerability they can search for the vulnerability using the CVE ID and apply the required remedies with any patch download if required);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>
---	---

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Exploit status:**

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

**Vulnerability Age:**


Vulnerability Manager Plus lets you calculate the age of a vulnerability either from the date on which the vulnerability is published or from the date on which it is discovered in your network. Letting a vulnerability reside in your network for a longer time is an indication of weak security. Therefore, vulnerability age must be taken into consideration while prioritizing vulnerabilities.

Using the above mentioned parameters, Vulnerabilities can be assessed and prioritized in many ways depending on your needs. It is advisable to use a combination of parameters to prioritize vulnerabilities. You can perform the entire operation of [vulnerability assessment](#) and remediation directly from the Vulnerability Manager Plus console.


<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15**


**U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Severity levels:**

Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability.

**Critical:**

Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first.

**Important:**

Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers.

**Moderate:**

Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS).

**Low:**

Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited.

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<div><div>Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)<div>Back to list</div></div><div><div><div><div><div><div>Vulnerability Name</div><div>:</div><div>Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)</div></div><div><div>Severity</div><div>:</div><div>Important</div></div><div><div>Exploits</div><div>:</div><div>Not available</div></div><div><div>CVE ID</div><div>:</div><div>CVE-2024-4331,CVE-2024-4368</div></div><div><div>Solution</div><div>:</div><div>MicrosoftEdgeEnterprise_124.0.2478.80_X64.msi</div></div><div><div>Published Date</div><div>:</div><div>03/05/2024</div></div><div><div>Updated Date</div><div>:</div><div>03/05/2024</div></div></div></div></div><div><p><b>Disclaimer:</b> This webpage is intended to provide you information about vulnerability announcement for certain specific software products. The information is provided "As Is" without warranty of any kind. The links provided point to pages on the vendors websites. You can get more information by clicking the links to visit the relevant pages on the vendors website.</p><p><a href="https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253712.html">https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253712.html</a></p></div></div></div>
--	---

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<div><div>Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)<div>Back to list</div></div><div><div><div><div><div><div>Vulnerability Name</div><div>:</div><div>Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)</div></div><div><div>Severity</div><div>:</div><div>Critical</div></div><div><div>Exploits</div><div>:</div><div>Not available</div></div><div><div>CVE ID</div><div>:</div><div>CVE-2022-0778,CVE-2022-21712</div></div><div><div>CVSS 3.0</div><div>:</div><div>9.1 (I:N/AV:N/AC:L/S:U/PR:N/A:H/UI:N/C:H)</div></div><div><div>Solution</div><div>:</div><div><a href="#">duoauthproxy-6.4.0.exe</a></div></div><div><div>Published Date</div><div>:</div><div>03/05/2024</div></div><div><div>Updated Date</div><div>:</div><div>03/05/2024</div></div></div></div></div><div><div><b>Disclaimer:</b> This webpage is intended to provide you information about vulnerability announcement for certain specific software products. The information is provided "As Is" without warranty of any kind. The links provided point to pages on the vendors websites. You can get more information by clicking the links to visit the relevant pages on the vendors website.</div><div><a href="https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253706.html">https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253706.html</a></div></div></div></div>
--	--

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p>  To remediate specific vulnerabilities</p> <ol style="list-style-type: none"> <li>1. Navigate to <b>threats&gt; software vulnerabilities</b>.</li> <li>2. In the "<b>Search by CVE ID</b>" field, specify the CVE IDs of the vulnerabilities you want to fix.</li> <li>3. Now selected the specific vulnerabilities and click on "<b>Install patches</b>" to create a manual deployment task.</li> <li>4. For further steps, refer to: <a href="https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html">Manually deploying patches to computers</a>.</li> </ol> <p><a href="https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html">https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html</a></p>
<p>said first occurrence of the first severity includes an incident and said second occurrence of the second severity includes an event;</p> <p>said second occurrence is reported differently than the first occurrence by not being reported;</p>	<p>ManageEngine discloses that <i>said first occurrence of the first severity includes an incident and said second occurrence of the second severity includes an event; said second occurrence is reported differently than the first occurrence by not being reported</i>; (e.g., the vulnerabilities identified by the Vulnerability Manager Plus will be stored in the Central Vulnerability Database wherein the database also provides every vulnerability with a CVE ID which is unique to every vulnerability so that in case a user want to access and apply patches for a specific vulnerability they can search for the vulnerability using the CVE ID and apply the required remedies with any patch download if required);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

| Exploit status:

This parameter displays whether an exploit code is available for the vulnerability or not. Vulnerabilities for which the exploit code have been disclosed are at a high-risk of being exploited. Exploit-code-available vulnerabilities with critical severity levels must be prioritized and eliminated at first.

| Vulnerability Age:

Vulnerability Manager Plus lets you calculate the age of a vulnerability either from the date on which the vulnerability is published or from the date on which it is discovered in your network. Letting a vulnerability reside in your network for a longer time is an indication of weak security. Therefore, vulnerability age must be taken into consideration while prioritizing vulnerabilities.

Using the above mentioned parameters, Vulnerabilities can be assessed and prioritized in many ways depending on your needs. It is advisable to use a combination of parameters to prioritize vulnerabilities. You can perform the entire operation of [vulnerability assessment](#) and remediation directly from the Vulnerability Manager Plus console.

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

Latest Vulnerabilities

Microsoft Vulnerabilities

Third Party Vulnerabilities

Web Server Vulnerabilities

DB Server Vulnerabilities

Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Severity levels:**

Vulnerabilities are classified into four severity levels ranging from low to critical based on its impact and exploitability.

**Critical:**

Vulnerabilities in the this range are easily exploitable and can result in root-level compromise of servers, remote code execution, information disclosure, etc. These vulnerabilities inflict great damage to the organization, therefore should be prioritized and remediated first.

**Important:**

Vulnerability that falls under this range are quite difficult to exploit but exploitation of them could result in significant data loss or downtime. Therefore, these vulnerabilities should be remediated once all the critical vulnerabilities are removed from your systems and servers.

**Moderate:**

Vulnerabilities in the medium range requires social engineering, or an access to the local network to be exploited. Even when exploited, these vulnerabilities have very limited access and, to the maximum extent, can cause Denial-of-service (DoS).

**Low:**

Vulnerabilities in the low range typically have tiny or no impact on an organization's business and may require local or physical system access to be exploited.

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The interface includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'. The main content area is divided into sections for 'Name and Description', 'Install Patch', 'List of Patches', 'Scheduler Settings', 'Deployment Rule', 'Deployment Settings', 'Define Targets', and 'Execution Settings'.

**Name and Description:** The 'Name' field is set to 'MyConfiguration070'. There is an 'Add Description' link.

**Install Patch:** The 'Operation Type' is set to 'Install Patch'. Below this is a table listing patches.

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16345	Security Update for Windows 8 (KB3010788)	May Require	Security Updates	Approved	1	0	X
19904	Security Update for Windows 8 (KB3121212)	May Require	Security Updates	Approved	1	0	X

**Scheduler Settings:** Includes checkboxes for 'Install After' and 'Do not apply this configuration after the time specified below'. There is a checkbox for 'Continue deployment even if some patches cannot be downloaded' with a note: 'Note: If the failed patches are successfully redownloaded, they will be installed in the subsequent refresh cycle (within deployment window)'.

**Deployment Settings:** The 'Apply Deployment Policy' dropdown is set to 'Select Policy'. There is a 'Create New Policy' link.

**Define Targets:** The 'Target 1' is set to 'Remote Office/Domain'. Below this, there are filters for 'Filter Computers based on' (set to 'Computer'), 'Exclude Target' (set to 'Domain'), and 'Domain' (set to 'Select').

**Execution Settings:** Labeled as '(Optional)'.

**Update Vulnerability DB:** A button labeled 'Update Now' is present, with a note 'Last Update Time: Jul 27, 2023 10:02 AM'.

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

This integrated vulnerability and patch management approach eliminates the need for multiple agents, disparity in data transferred between multiple solutions, potential delays in remediation, unnecessary silos, and false positives. Vulnerability Manager Plus also empowers you with a [separate patch management module](#) to completely automate your regular patching schedules, enabling your IT staff to spend more time on assessing and prioritizing high-risk vulnerabilities.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Other features****Firewall Reports**

Get a slew of security and traffic reports to assess the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.

**Firewall Log Management**

Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.

**Firewall Alerts**

Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.

**Firewall Compliance Management**

Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.

**Real-time Bandwidth Monitoring**

With live bandwidth monitoring, you can identify the abnormal sudden shoot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.

**Manage Firewall Service**

MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Measure, Track, analyse your progress with insightful reports:

Your entire [vulnerability management](#) program becomes futile if you can't evaluate your efforts and understand your security stance. Vulnerability manager Plus brings you massive collection of pre-defined, insightful reports that you can use to scrutinize your network security, communicate risks, track progress and report on security regulations to executives.

These reports comes in different formats to cater to your needs. You can also schedule reports to security executives, administrators and enterprise risk management teams with just a click from the console.

### Executive asset summary:

Get an overview of the assets you manage and insights on critical assets that should be prioritized.

### Executive vulnerability summary:

The executive vulnerability summay report helps you gain detailed information on vulnerabilities, security misconfigurations, high risk softwares, vulnerable ports and webserver flaws in your network.

### Executive patch summary:

Executive patch summary report provides an overview of missing patches and deployments that help you track the measures taken to safeguard your enterprise.

### Threat priority report:

The threat priority report gives you a prioritized list of the assets, vulnerabilities, misconfigurations and other threats that are more likely to be exploited and needs immediate attention.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/insightful-reports.html>

| Pre-defined reports - Dig a level deeper into your security exposure.

Patch reports:

**Vulnerable patches:**

This report displays a list of all the missing patches in the network and details on affected systems for every patch that is listed.

**Supported patches:**

This report delivers details on all the patches released by Microsoft Corporation irrespective of whether these patches have a relation to your network or not. This report will be of absolute use when you plan to upgrade the systems in your network by installing the latest applications/ updates available for the application.

**Missing patches awaiting approval:**

This report will list down all the tested patches that are missing in your endpoints but have not been approved for deployment.

**Remote office patch summary:**

The Remote Office Patch Summary Report lists down the number of missing patches, installed patches, applicable patches, healthy systems, vulnerable systems, highly vulnerable systems and managed computers by your remote offices.

<https://www.manageengine.com/vulnerability-management/insightful-reports.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<p>said first technique for setting or modifying the policy includes just setting the policy;</p> <p>said first technique for setting or modifying the policy includes just setting the policy, and said policy is associated with at least one of a policy template, a custom policy, or standardized template;</p>	<p>ManageEngine discloses that <i>said first technique for setting or modifying the policy includes just setting the policy</i> (e.g., a policy for changing the patches or modifying or adding any policies in the firewall or vulnerability manager of the system); <i>said first technique for setting or modifying the policy includes just setting the policy, and said policy is associated with at least one of a policy template, a custom policy, or standardized template</i> (e.g., directly blocking or restricting the use of files or software that is found vulnerable to a threat based on the predefined patch);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>
--	--

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

**High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of misconfigurations. A filter dropdown is open, showing categories like Antivirus Protection, User Account Management, Windows Firewall (highlighted with a red box), Password Policy, SSL and TLS Security, and Chrome Security Hardening. The list of misconfigurations includes entries like 'Geolocation is enabled to track', 'TLSv1.1 protocol is enabled', 'Administrative Shares enabled', 'Data Execution Prevention is not enabled', 'Maximum Password age is not configured to 45 days', 'Secure logon (Ctrl+Alt+Delete logon) is not enabled', 'Antivirus (not considering Windows Defender) not installed', 'Account lockout duration is not configured to 1440 minutes', 'Built-in Administrator Account is not disabled', 'Folder shares are assigned to everyone group', 'Windows firewall disabled/ No third-party firewall pre...' (highlighted with a red box), and 'Outdated plugins are allowed to run'. The 'Windows firewall disabled' entry is marked as 'Critical' and affects 1 system.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	Security Hardening	2	Info
TLSv1.1 protocol is enabled	TLS Security	1	Info
Administrative Shares enabled	Permission Management	3	Info
Data Execution Prevention is not enabled	Security Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus web interface. The main panel shows a list of misconfigurations. A modal window titled 'Misconfiguration Details' is open, showing the following information:

Field	Value
Name	Data Execution Prevention is not enabled
Description	DEP/NX (Data Execution Prevention/ No Execution) marks the memory pages as executable and non-executable. Further, it detects the presence of executable data in non-executable memory page and terminates the execution of malicious code placed by an attacker. DEP is a highly effective security feature that must be enabled in your network computers.
Severity	Critical
Misconfigured in Domain GPO	No
<b>Solution</b>	
<b>Resolution</b>	<b>Deploy Secure Configuration</b>
Post Deployment Issues	Some legacy applications are not compatible with DEP (Data Execution Prevention) and might crash when DEP is enabled. You can exclude such applications from DEP settings. Also, the potential impact varies depending on the importance of applications and services that are dependent on DEP (attach an error kb on how to exclude applications from DEP settings)

The 'Resolution' field is highlighted with a red box. The interface also shows a list of other misconfigurations on the right side, including 'Windows Firewall' and 'Chrome Security Hardening'.

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Other features****Firewall Reports**

Get a slew of security and traffic reports to assess the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.

**Firewall Log Management**

Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.

**Firewall Alerts**

Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.

**Firewall Compliance Management**

Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.

**Real-time Bandwidth Monitoring**

With live bandwidth monitoring, you can identify the abnormal sudden shoot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.

**Manage Firewall Service**

MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the ManageEngine Vulnerability Management console. The left sidebar contains navigation options: Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is titled 'Install/Uninstall Windows Patch (Computer)' and includes sections for Name and Description, Install Patch, List of Patches, Scheduler Settings (optional), Deployment Rule, Deployment Settings, Define Targets, and Execution Settings (optional).

**List of Patches:**

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16340	Security Update for Windows 8 KB3032758	May Require	Security Update	Approved	1	0	R
27504	Security Update for Windows 8 KB3032758	May Require	Security Update	Approved	1	0	R

**Define Targets:**

Target 1: Remote Office Domain, Local Office

Filter Computers based on: Computer (Selected), Domain (DOWNSIDE)

Exclude Target: Domain (Selected)

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot displays the ManageEngine Vulnerability Assessment interface. The left sidebar shows a navigation menu with categories like 'System Health Summary', 'Highly Vulnerable Systems (3)', 'Vulnerable Systems (1)', 'Healthy Systems (6)', 'System Health Policy', 'Managed Systems', 'Scan Systems (13)', 'By Patches', 'By Vulnerabilities (7)', 'By Misconfigurations (8)', 'By Web Server Misconfiguration (5)', 'By High Risk Software (7)', 'Attention Required', and 'Windows 10 EOL Systems'. The main content area is titled 'suraj-7073' and shows a 'Vulnerabilities' tab. Below this, there are three sections: 'Software Vulnerabilities', 'Server Vulnerabilities', and 'Zero-day Vulnerabilities'. The 'Server Vulnerabilities' section is active, showing a table of vulnerabilities. The table has columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. There are three rows of vulnerabilities listed, all with an exploit status of 'Not available' and a patch availability of 'Not available'. The CVSS 3.0 scores are 7.5, 7.5, and 6.9, while the CVSS 2.0 scores are 5.0, 5.0, and 7.5. At the bottom of the table, it shows '1 - 3 of 3' and a dropdown menu set to '30'.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527/CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329/CVE-2020-9484/CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

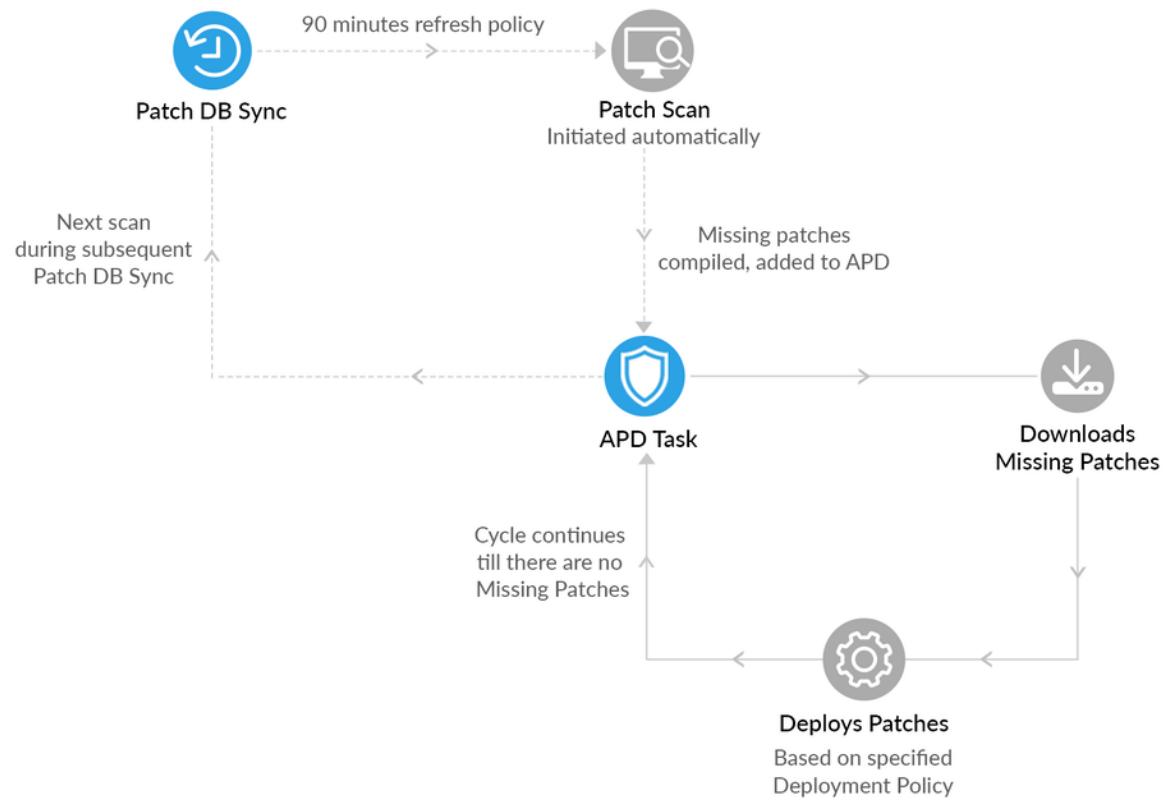
- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Automate Patch Deployment Task Workflow**



<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**| Need for Automated Patch Deployment:**

With the steady rise in attack vendors and frequency of attacks, it is mandatory to keep all your enterprise endpoints up to date and round the clock patched. The best way to address this problem, is to have a systematic and automated solution that manages multiple OSs and third party application patches effectively.

The **Automate Patch Deployment** (APD) feature provides system administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention required.

**| Automate Patch Deployment (APD) workflow has been enhanced!**

To keep up with cyber industry's security demands and requests from a few customers, ManageEngine's **Patch Management** module has undergone a few enhancements in the '**Automated Patch Deployment**'(APD) functionality. We will shed light on what's new with the latest APD feature.

<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Benefits of new-feel Automated Patch Deployment</b></p> <ol style="list-style-type: none"> <li>1. Deployments are fast, and security is tightened due to the readily available patches for deployment.</li> <li>2. All the approved patches will be deployed in the very next deployment window immediately after their download. There's no need to wait for the next APD scheduler to invoke the deployment.</li> <li>3. Whenever the computer in the network goes offline and encounters the network connectivity again, there could be new vulnerabilities and patches that the computer be missing. In the new APD, when the agent comes into contact with the server, it gets automatically scanned in the next refresh cycle, the missing patches are detected and updated in the server. The agent deploys them in the subsequent refresh cycle during the deployment window. Hence, there is no need to worry about the agent contact time and its prolonged vulnerable status. In the old APD, patch installation might be delayed because the agent contacted the server only after APD schedule.</li> <li>4. Deployment in agent continues until it gets zero missing patches for the APD criteria.</li> <li>5. In the new APD, you can also see the history of patching in a more detailed view.</li> </ol> <p><a href="https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html">https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html</a></p>
<p>said second technique for reacting to the packets is carried out utilizing a firewall;</p> <p>said occurrence mitigation includes at least one of</p>	<p>ManageEngine discloses that <i>said second technique for reacting to the packets is carried out utilizing a firewall</i> (e.g., the packets are analyzed on the firewall of the ManageEngine); <i>said occurrence mitigation includes at least one of removing the one or more actual vulnerabilities, or reducing an effect of a detected occurrence</i> (e.g., the detected vulnerabilities on the firewall are audited and removed using the remedies and policies defined in the Firewall Rule Management wherein the policies can be user-defined or preinstalled in the software);</p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

removing the one or more actual vulnerabilities, or reducing an effect of a detected occurrence;

**Note:** See, for example, the evidence below (emphasis added, if any):

### See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

### High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

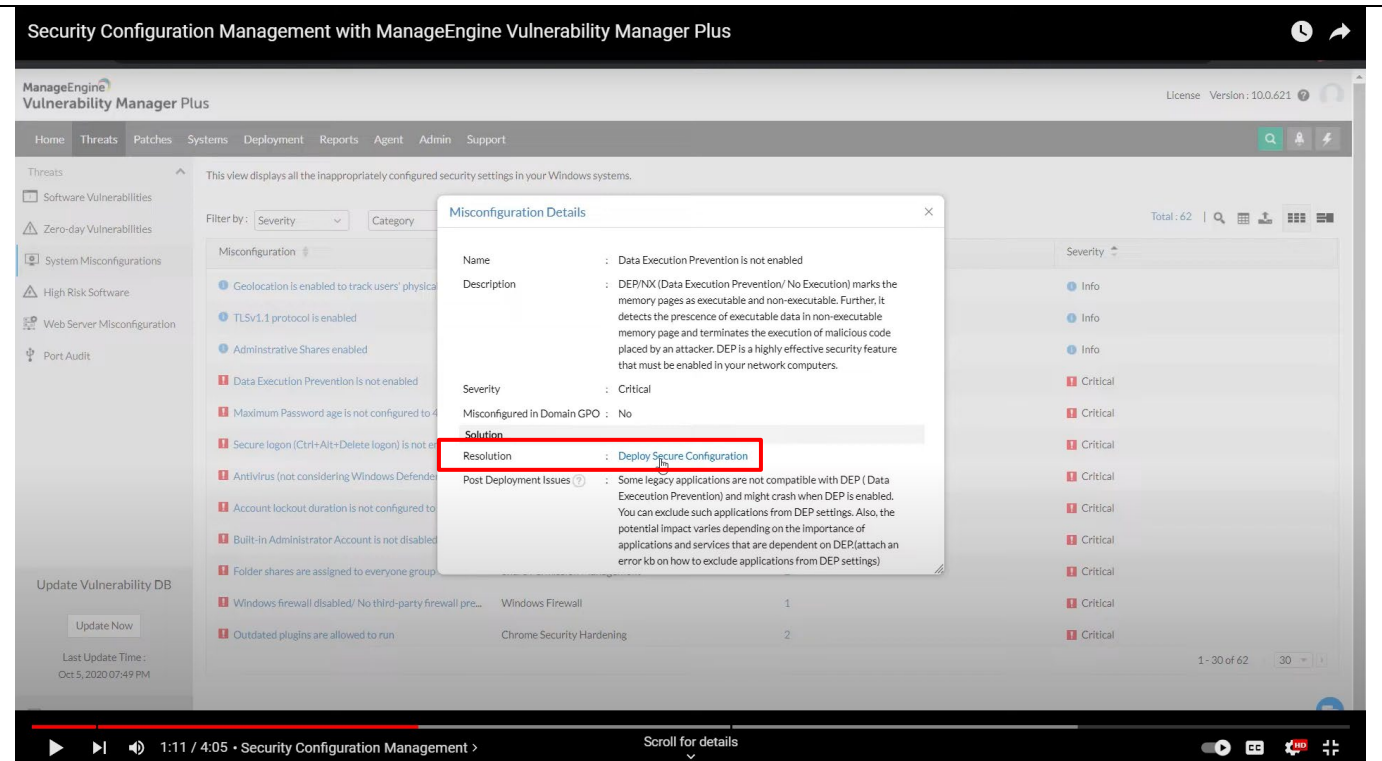
<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Home, Threats, Patches, Systems, Deployment, Reports, Agent, Admin, and Support. The main content area is titled 'Security Configuration Management with ManageEngine Vulnerability Manager Plus'. It shows a list of misconfigurations in Windows systems. A filter dropdown is open, showing 'Category' with 'Windows Firewall' selected. The table below lists various misconfigurations, their categories, the number of affected systems, and their severity levels. One entry, 'Windows firewall disabled/ No third-party firewall pre...', is highlighted with a red box and marked as 'Critical'.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	Windows Firewall	2	Info
TLSv1.1 protocol is enabled	Windows Firewall	1	Info
Administrative Shares enabled	Windows Firewall	3	Info
Data Execution Prevention is disabled	Windows Firewall	4	Critical
Maximum Password age is not configured to 45 days	Windows Firewall	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Windows Firewall	1	Critical
Antivirus (not considering Windows Defender) not installed	Windows Firewall	1	Critical
Account lockout duration is not configured to 1440 minutes	Windows Firewall	2	Critical
Built-in Administrator Account is not disabled	Windows Firewall	2	Critical
Folder shares are assigned to everyone group	Windows Firewall	2	Critical
<b>Windows firewall disabled/ No third-party firewall pre...</b>	<b>Windows Firewall</b>	<b>1</b>	<b>Critical</b>
Outdated plugins are allowed to run	Windows Firewall	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

## Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Other features****Firewall Reports**

Get a slew of security and traffic reports to assess the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.

**Firewall Log Management**

Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.

**Firewall Alerts**

Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.

**Firewall Compliance Management**

Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.

**Real-time Bandwidth Monitoring**

With live bandwidth monitoring, you can identify the abnormal sudden shoot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.

**Manage Firewall Service**

MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The left sidebar contains navigation options: Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is divided into several sections:

- Name and Description:** A text field labeled 'Name' with the value 'NoConfiguredPDS' and a link to 'Add Description'.
- Install Patch:** A section with 'Operation Type' set to 'Install Patch' (radio button selected) and 'General Patch' (radio button unselected).
- Table of Patches:** A table listing available patches for installation.
 

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16340	Security Update for Windows 8 KB3033970	May Require	Security Update	Approved	1	0	W
27504	Security Update for Windows 8 KB3033970	May Require	Security Update	Approved	1	0	W
- Schedule Settings (Optional):** Includes checkboxes for 'Install Only' and 'Do not apply Windows configuration after the time specified below'. A 'Deployment Rule' section contains a checkbox for 'Continue deployment even if some patches cannot be downloaded'.
- Deployment Settings:** Includes a dropdown for 'Apply Deployment Policy' set to 'Select Policy' and a link to 'Create Policy'.
- Define Target:** A section for selecting targets, including 'Remote Office Domain' and 'Local Office'. A filter for 'Filter Computers based on' is set to 'Computer' with the value 'SECURITY-WIN-02'. An 'Exclude Target' dropdown is set to 'Select'.
- Execution Settings (Optional):** A section for configuring execution parameters.

At the bottom left, there is a button 'Update Vulnerability DB' and a timestamp 'Last Update Time: JUL 20 10:03 AM'.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

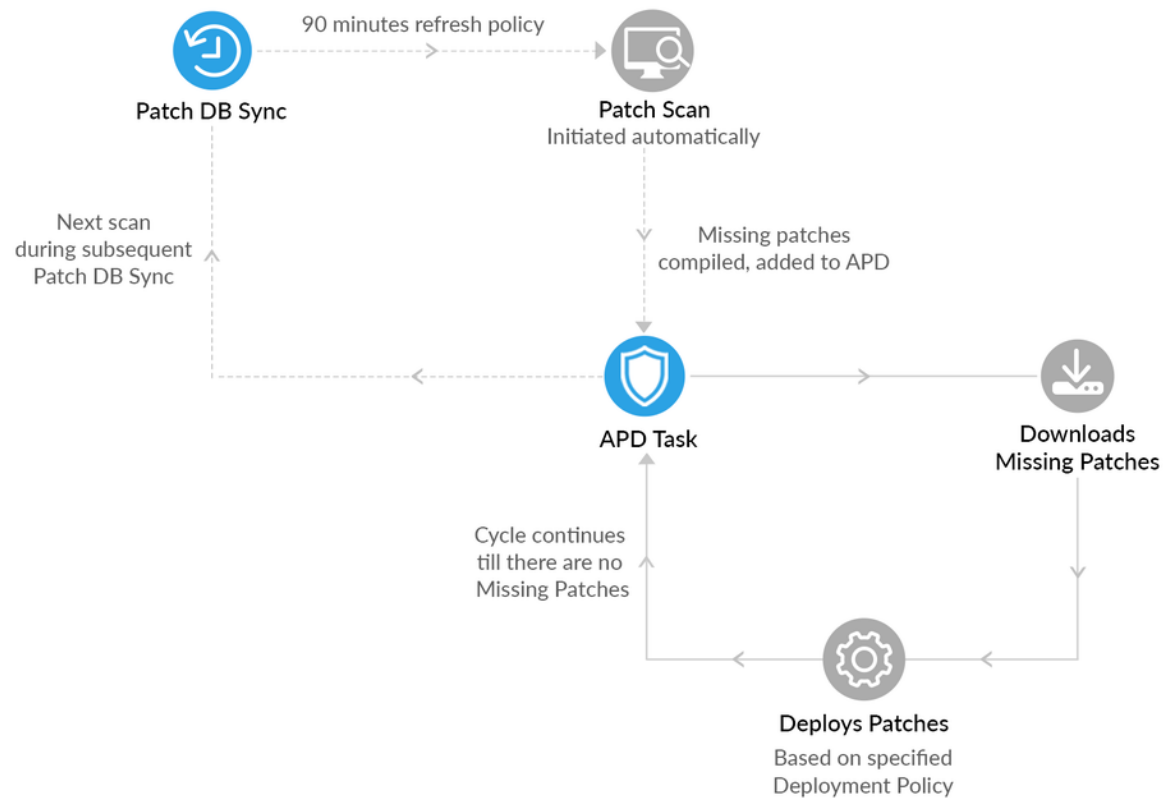
Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot displays the ManageEngine Vulnerability Assessment interface. The sidebar on the left contains navigation links for System Health Summary, Highly Vulnerable Systems (3), Vulnerable Systems (1), Healthy Systems (6), System Health Policy, Managed Systems, Scan Systems (13), By Patches, By Vulnerabilities (7), By Misconfigurations (8), By Web Server Misconfiguration (5), By High Risk Software (7), Attention Required, and Windows 10 EOL Systems. The main content area shows a drilled-down view for system 'suraj-7073'. It includes tabs for Summary, Installed Software, Vulnerabilities, Patches, Security Config, and Port Audit. The Vulnerabilities tab is active, showing a table of vulnerabilities categorized by Web, Database, and Content Management Systems. The table lists vulnerabilities with details such as CVE IDs, file paths, exploit status, and patch availability.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527/CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329/CVE-2020-9484/CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Automate Patch Deployment Task Workflow**

<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**| Need for Automated Patch Deployment:**

With the steady rise in attack vendors and frequency of attacks, it is mandatory to keep all your enterprise endpoints up to date and round the clock patched. The best way to address this problem, is to have a systematic and automated solution that manages multiple OSs and third party application patches effectively.

The **Automate Patch Deployment** (APD) feature provides system administrators the ability to deploy patches missing in their network computers automatically, without any manual intervention required.

**| Automate Patch Deployment (APD) workflow has been enhanced!**

To keep up with cyber industry's security demands and requests from a few customers, ManageEngine's **Patch Management** module has undergone a few enhancements in the '**Automated Patch Deployment**' (APD) functionality. We will shed light on what's new with the latest APD feature.

<https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Benefits of new-feel Automated Patch Deployment</b></p> <ol style="list-style-type: none"> <li>1. Deployments are fast, and security is tightened due to the readily available patches for deployment.</li> <li>2. All the approved patches will be deployed in the very next deployment window immediately after their download. There's no need to wait for the next APD scheduler to invoke the deployment.</li> <li>3. Whenever the computer in the network goes offline and encounters the network connectivity again, there could be new vulnerabilities and patches that the computer be missing. In the new APD, when the agent comes into contact with the server, it gets automatically scanned in the next refresh cycle, the missing patches are detected and updated in the server. The agent deploys them in the subsequent refresh cycle during the deployment window. Hence, there is no need to worry about the agent contact time and its prolonged vulnerable status. In the old APD, patch installation might be delayed because the agent contacted the server only after APD schedule.</li> <li>4. Deployment in agent continues until it gets zero missing patches for the APD criteria.</li> <li>5. In the new APD, you can also see the history of patching in a more detailed view.</li> </ol> <p><a href="https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html">https://www.manageengine.com/patch-management/help/automate-patch-deployment-task.html</a></p>
<p>said reacting to packets involves at least one of dropping, blocking, or redirecting;</p> <p>said occurrence mitigation is carried out for protecting at</p>	<p>ManageEngine discloses that <i>said reacting to packets involves at least one of dropping, blocking, or redirecting</i> (e.g., remedies to remove vulnerabilities); <i>said occurrence mitigation is carried out for protecting at least one particular aspect of one or more of the networked devices</i> (e.g., said remedies applied on the network devices or endpoints to remove vulnerabilities), <i>where the one or more of the networked devices include at least one of a client or a server</i> (e.g., the networked devices are endpoints in the architecture which are identified as user devices or end equipment or remote devices that requires</p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

least one particular aspect of one or more of the networked devices, where the one or more of the networked devices include at least one of a client or a server, and the at least one particular aspect includes at least one of an operating system or an application;

vulnerability protection within the network downloaded on a central server and applied on the complete network), *and the at least one particular aspect includes at least one of an operating system or an application* (e.g., vulnerabilities on the network devices include software-based vulnerabilities like, end of life software, virus attack, malware attack, remote desktop sharing etc. that are operated on the operating system of the devices including updates of the operating system);

**Note:** See, for example, the evidence below (emphasis added, if any):

### Enterprise vulnerability management software

Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step [vulnerability management](#) in your enterprise with Vulnerability Manager

Plus

#### Scan



Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.

#### Assess



Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.

#### Manage



Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS>

**Comprehensive vulnerability scanning**

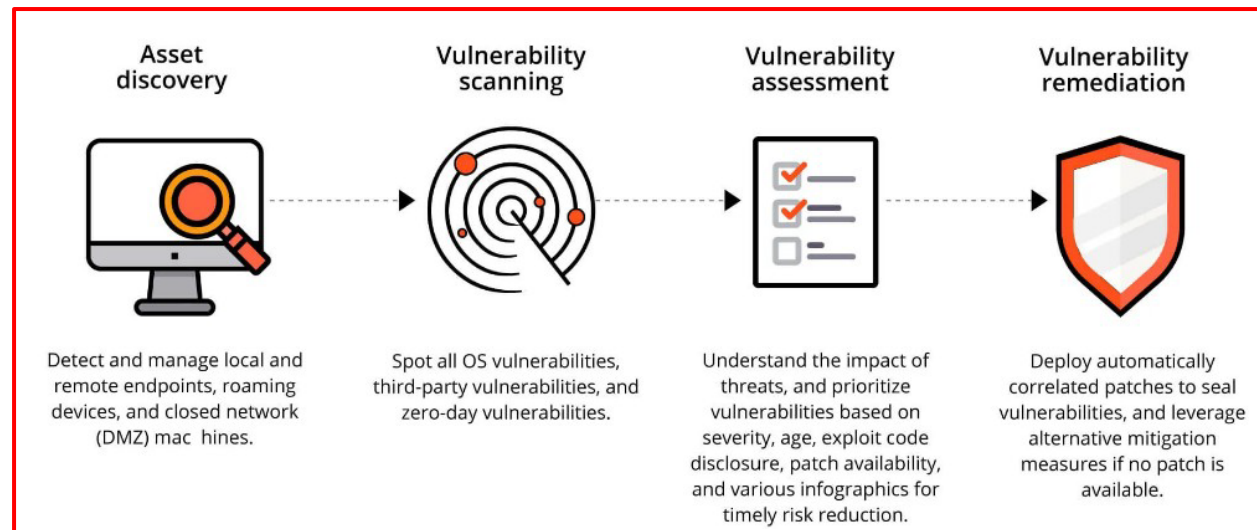
Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****What are the 4 steps in vulnerability assessment?**

Vulnerability Manager Plus is a well-rounded vulnerability assessment tool that regularly scans your network for vulnerabilities, delivers insights into risk, and helps close the vulnerability management loop instantly with direct remediation from the console.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar lists various threat categories, with 'Zero-day Vulnerabilities' highlighted. The main panel displays a table of zero-day vulnerabilities. The table has columns for 'Threats', 'Threat Category', 'Affected Systems', and 'Action'. The data rows include Google Chrome (x64) (78.0.3904.87), 2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20..., and 2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200... Each row shows a 'Fix' button. The interface also includes a search bar, a filter dropdown, and a 'Total: 5' indicator.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

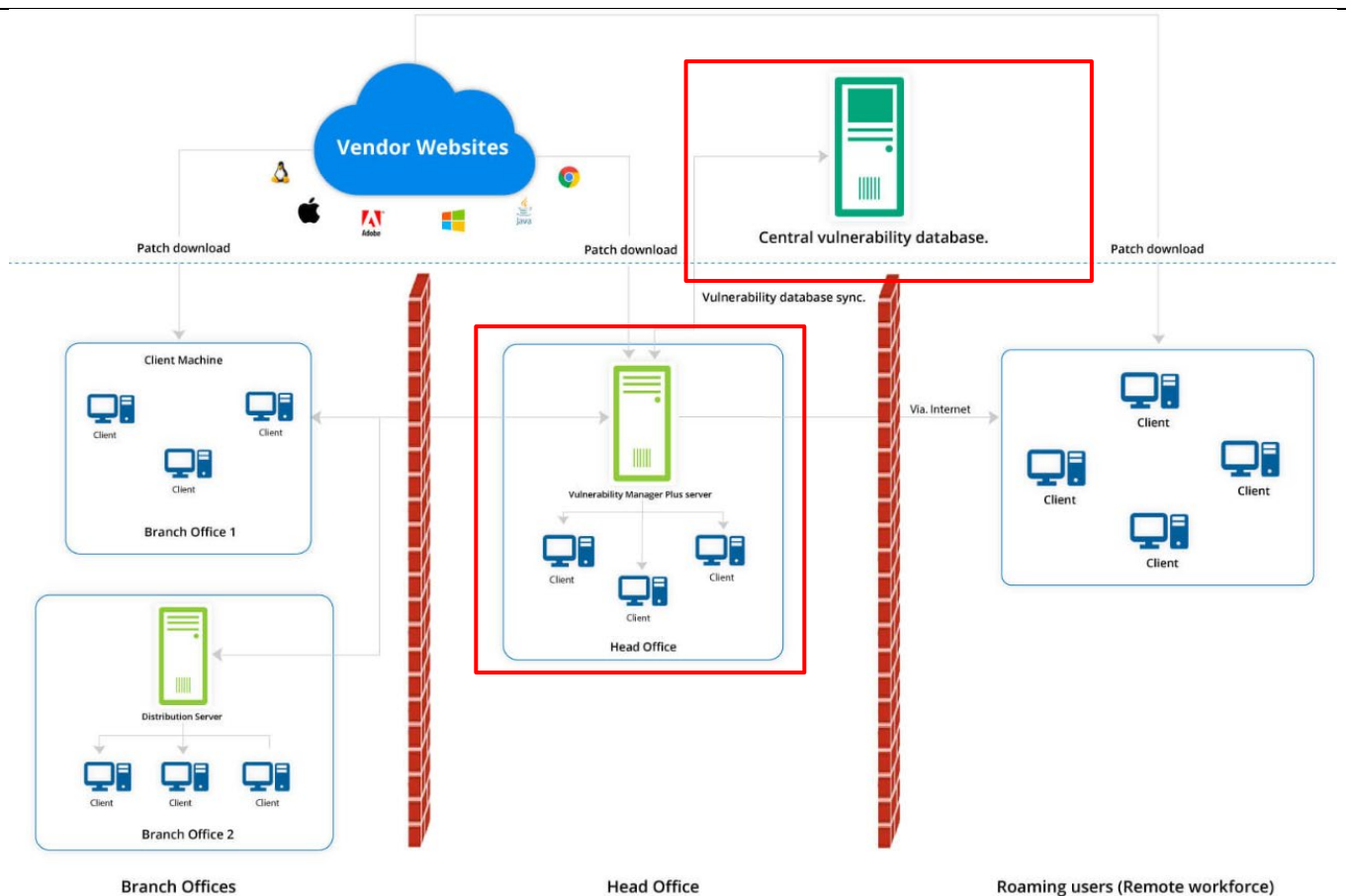
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the *Vulnerability Manager Plus* pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****See what matters most at a glimpse with dashboard widgets**

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary


Zero-day  
vulnerabilities

Vulnerability  
Age Matrix

Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

**High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities		Vulnerable Software			
Vulnerabilities		Affected Systems	Exploit Status	Software Name	
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	1	Available	Windows 8.1 Enterprise Edition (x64)	
				Windows 8.1 Home Basic Edition (x64)	
				Windows 8.1 Home Premium Edition (x64)	
				Windows 8.1 Professional Edition (x64)	

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The interface includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'. The main content area is divided into sections for 'Name and Description', 'Install Patch', 'List of Patches', 'Scheduler Settings', 'Deployment Rule', 'Deployment Settings', 'Define Targets', and 'Execution Settings'.

**Name and Description:** The 'Name' field is set to 'MyConfiguration070'. There is an 'Add Description' link.

**Install Patch:** The 'Operation Type' is set to 'Install Patch'. Below this is a table listing patches.

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16345	Security Update for Windows 8 (KB3010788)	May Require	Security Updates	Approved	1	0	X
19904	Security Update for Windows 8 (KB3121212)	May Require	Security Updates	Approved	1	0	X

**Scheduler Settings:** Includes checkboxes for 'Install After' and 'Do not apply this configuration after the time specified below'. There is a checkbox for 'Continue deployment even if some patches cannot be downloaded' with a note: 'Note: If the failed patches are successfully redownloaded, they will be installed in the subsequent refresh cycle (within deployment window)'.

**Deployment Settings:** The 'Apply Deployment Policy' dropdown is set to 'Select Policy'. There is a 'Create/Modify Policy' link.

**Define Targets:** The 'Target 1' is set to 'Remote Office/Domain'. Below this, there are filters for 'Filter Computers based on' (set to 'Computer') and 'Exclude Target' (set to 'Domain').

**Execution Settings:** This section is currently empty.

**Update Vulnerability DB:** A button labeled 'Update Now' is present, with a note 'Last Update Time: Jul 27, 2023 10:02 AM'.

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

This integrated vulnerability and patch management approach eliminates the need for multiple agents, disparity in data transferred between multiple solutions, potential delays in remediation, unnecessary silos, and false positives. Vulnerability Manager Plus also empowers you with a [separate patch management module](#) to completely automate your regular patching schedules, enabling your IT staff to spend more time on assessing and prioritizing high-risk vulnerabilities.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

ManageEngine Rounds off Its Endpoint Protection Platform with the Addition of Next Generation Antivirus Capability

Capability Added to Endpoint Central, its UEM Solution, to Tackle the Dynamic Threat Landscape

- Proactive, AI-based protection with real-time monitoring for known and unknown threats
- Unified approach promotes interoperability between IT functions, simplifying threat detection, investigation and remediation
- Download a 30-day, free trial of Endpoint Central at <https://mnge.it/NGAV>

<https://www.manageengine.com/news/manageengine-rounds-endpoint-protection-platform-addition-next-generation-antivirus-capability.html?meseach>

## **EXHIBIT 15**

### **U.S. Patent No 9,118,711 v. Zoho**

#### Benefits of Endpoint Central's NGAV

Endpoint Central uses a single, lightweight agent for its wide range of high-stakes capabilities like device life cycle management, remote troubleshooting, user experience management and endpoint security.

Apart from reducing organizations' IT footprints, this unified approach offers:

- **A wide scope for remediation policies:** Security teams can apply necessary patches, quarantine affected devices from the internet and intranet, force login credential resets, revert devices to their IT-approved baseline versions and remove vulnerable applications.
- **Seamless incident investigation:** Built-in remote troubleshooting and system management capabilities offer instant and thorough incident investigation of quarantined devices.
- **Feedback loops for bolstering the security posture:** Security policies can be continuously updated based on threats detected by the NGAV engine, constantly enhancing the cybersecurity posture.

ManageEngine has been in the IT management market for over 20 years and has built a strong foundation of IT management and security capabilities from the ground up. The NGAV addition to Endpoint Central is a move to strengthen endpoint security within the company's comprehensive portfolio of cybersecurity solutions.

"We aim to offer an AI-powered, unified, end-to-end platform for the digital enterprise in which cyber resilience is of paramount importance," added Venkatachalam. "The platform will enable customers to devise and implement a comprehensive security strategy by building workflows across multiple ManageEngine security offerings, automating threat detection, threat responses and incident investigation."

<https://www.manageengine.com/news/manageengine-rounds-endpoint-protection-platform-addition-next-generation-antivirus-capability.html?mesearch>

#### **Virus, Attack, Security, and Spam Reports from Firewall Logs**

##### **Detailed Security, Virus, Attack and Spam Analysis**

Firewall Analyzer includes instant reports on **viruses**, **attacks** and **security** breach in your network. These reports instantly show you the **viruses active** on the network, the hosts that have been affected, and more. With these reports it is easier for IT to do business risk assessment, detect problems and resolve them as soon as they are found.

<https://www.manageengine.com/products/firewall/firewall-virus-report.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p><b>Virus Reports</b></p> <p>Virus reports give in-depth information on virus attacks, hosts infected, severity of the attack, subtype, and more. With drillable details to the raw log level on top viruses and top protocols used by viruses, the complete details of the virus related raw log is available. The raw log message make troubleshooting and problem resolution faster and more efficient.</p> <p><a href="https://www.manageengine.com/products/firewall/firewall-virus-report.html">https://www.manageengine.com/products/firewall/firewall-virus-report.html</a></p>
<p>said particular actual vulnerability is at least one of the actual vulnerabilities;</p> <p>said certain actual vulnerability is at least one of the actual vulnerabilities;</p> <p>said particular actual vulnerability is the certain actual vulnerability;</p> <p>said particular occurrence is the certain occurrence;</p> <p>said particular occurrence includes the first occurrence;</p>	<p>ManageEngine discloses that <i>said particular actual vulnerability</i> (e.g., unknown/potential vulnerabilities to the devices) <i>is at least one of the actual vulnerabilities</i> (e.g., known/existent vulnerabilities to the devices); <i>said certain actual vulnerability</i> (e.g., unknown/potential vulnerabilities to the devices) <i>is at least one of the actual vulnerabilities</i>; <i>said particular actual vulnerability is the certain actual vulnerability</i>; <i>said particular occurrence is the certain occurrence</i>; <i>said particular occurrence includes the first occurrence</i>; <i>said certain occurrence includes the first occurrence</i> (e.g., detection of different types of vulnerabilities can be different occurrences wherein the vulnerabilities can belong to different severity group); <i>said first and second techniques include remediation techniques</i> (e.g., remedies used to remove, block, restrict or delete a vulnerability are different remediation techniques); <i>said first occurrence includes an attack</i> (e.g., the attack can be on firewall , software, operating system, virus attack, etc. on the network devices or the Central server managing the network);</p> <p><b>Note:</b> See, for example, the evidence below (emphasis added, if any):</p>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

said certain occurrence includes the first occurrence;

said first and second techniques include remediation techniques;

said first occurrence includes an attack;

## 2) What is Vulnerability Scanning?

Vulnerability scanning is a security process that checks your computer systems to find any weaknesses or vulnerabilities that could be used by hackers to gain unauthorized access. It's like a thorough check-up for your network and software, where any potential security risks are identified and reported back to you so that you can take action to fix them. This helps to protect your organization's digital assets and ensures that sensitive information remains secure.

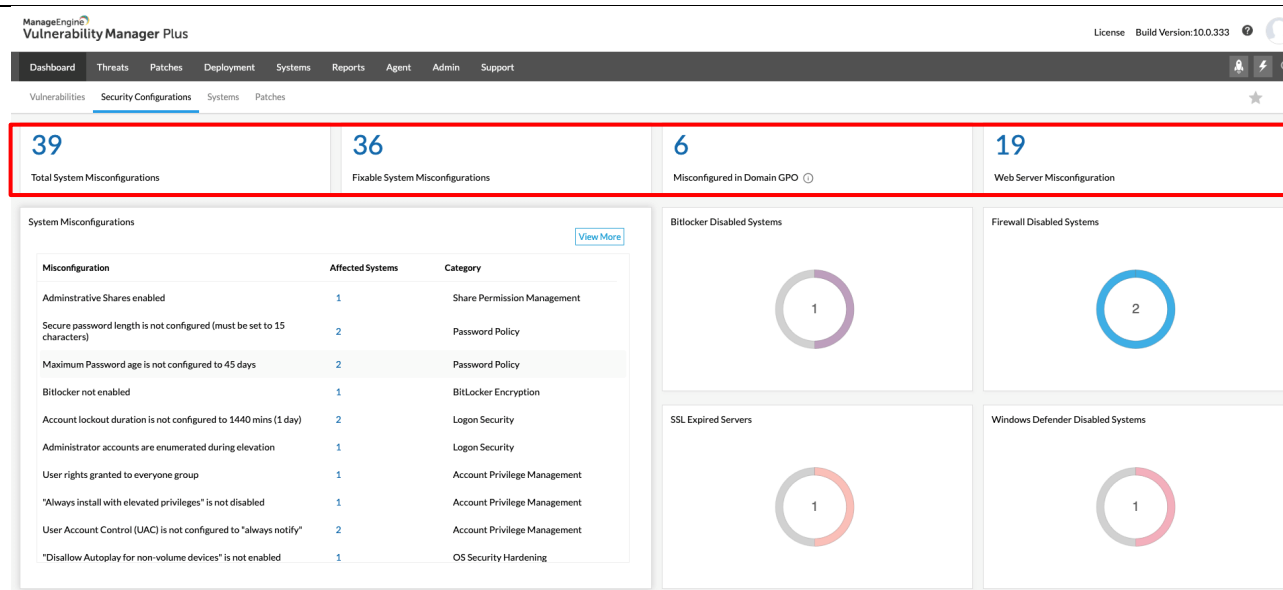
<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

## Comprehensive vulnerability scanning

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:






- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

				
Latest Vulnerabilities	Microsoft Vulnerabilities	Third Party Vulnerabilities	Web Server Vulnerabilities	DB Server Vulnerabilities

⌚ Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The top navigation bar includes links for Dashboard, Threats, Patches, Deployment, Systems, Reports, Agent, Admin, and Support. The left sidebar lists various threat categories, with 'Zero-day Vulnerabilities' highlighted. The main content area displays a table of zero-day vulnerabilities. The table has columns for Threats, Threat Category, Affected Systems, and Action. The data rows list specific vulnerabilities, including Google Chrome (x64) (78.0.3904.87) and various Internet Explorer security updates. Each row shows the threat category, the number of affected systems (1), and a 'Fix' button. A search bar at the top allows filtering by threat category or CVE ID. The bottom right corner shows pagination: 1-5 of 5, with a dropdown for 30 items per page.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****See what matters most at a glimpse with dashboard widgets**

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix

Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

**High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities		Vulnerable Software			
Vulnerabilities		Affected Systems	Exploit Status	Software Name	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)	

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

ManageEngine Rounds off Its Endpoint Protection Platform with the Addition of Next Generation Antivirus Capability

Capability Added to Endpoint Central, its UEM Solution, to Tackle the Dynamic Threat Landscape

- Proactive, AI-based protection with real-time monitoring for known and unknown threats
- Unified approach promotes interoperability between IT functions, simplifying threat detection, investigation and remediation
- Download a 30-day, free trial of Endpoint Central at <https://mnge.it/NGAV>

Benefits of Endpoint Central's NGAV

Endpoint Central uses a single, lightweight agent for its wide range of high-stakes capabilities like device life cycle management, remote troubleshooting, user experience management and endpoint security.

Apart from reducing organizations' IT footprints, this unified approach offers:

- **A wide scope for remediation policies:** Security teams can apply necessary patches, quarantine affected devices from the internet and intranet, force login credential resets, revert devices to their IT-approved baseline versions and remove vulnerable applications.
- **Seamless incident investigation:** Built-in remote troubleshooting and system management capabilities offer instant and thorough incident investigation of quarantined devices.
- **Feedback loops for bolstering the security posture:** Security policies can be continuously updated based on threats detected by the NGAV engine, constantly enhancing the cybersecurity posture.

ManageEngine has been in the IT management market for over 20 years and has built a strong foundation of IT management and security capabilities from the ground up. The NGAV addition to Endpoint Central is a move to strengthen endpoint security within the company's comprehensive portfolio of cybersecurity solutions.

"We aim to offer an AI-powered, unified, end-to-end platform for the digital enterprise in which cyber resilience is of paramount importance," added Venkatachalam. "The platform will enable customers to devise and implement a comprehensive security strategy by building workflows across multiple ManageEngine security offerings, automating threat detection, threat responses and incident investigation."

<https://www.manageengine.com/news/manageengine-rounds-endpoint-protection-platform-addition-next-generation-antivirus-capability.html?meseach>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<div data-bbox="617 261 1881 524"><p><b>Virus, Attack, Security, and Spam Reports from Firewall Logs</b></p><p><b>Detailed Security, Virus, Attack and Spam Analysis</b></p><p>Firewall Analyzer includes instant reports on <a href="#">viruses</a>, <a href="#">attacks</a> and <a href="#">security</a> breach in your network. These reports instantly show you the <a href="#">viruses active</a> on the network, the hosts that have been affected, and more. With these reports it is easier for IT to do business risk assessment, detect problems and resolve them as soon as they are found.</p></div> <div data-bbox="617 563 1892 764"><p><b>Virus Reports</b></p><p><a href="#">Virus reports</a> give in-depth information on virus attacks, <a href="#">hosts infected</a>, severity of the attack, subtype, and more. With drillable details to the raw log level on <a href="#">top viruses</a> and top protocols used by viruses, the complete details of the virus related raw log is available. The raw log message make troubleshooting and problem resolution faster and more efficient.</p></div> <p><a href="https://www.manageengine.com/products/firewall/firewall-virus-report.html">https://www.manageengine.com/products/firewall/firewall-virus-report.html</a></p>
--	---

EXHIBIT 15

U.S. Patent No 9,118,711 v. Zoho

	<div><div><div>Custom Report</div><div>Firewall Reports</div><div>Proxy Reports</div><div>API Access</div><div>General</div></div><div><div>Device Name</div><div>All Devices</div></div><div><div>Report Type</div><div>Security Reports</div><div>Virus Reports</div><div>Attack Reports</div><div>Spam Reports</div><div>Protocol Trend Reports</div><div>Traffic Trend Reports</div><div>Event Trend Reports</div><div>Admin Reports</div><div>VPN Trend Report</div><div>URL Report</div><div>Active VPN Trend</div></div></div> <div><div><div>Virus Reports</div><div>Resolve DNS</div></div><div><div>Top Virus Sending Hosts</div><div>Resolve DNS</div></div><div><div>Top Virus Affected Hosts</div><div>Resolve DNS</div></div></div> <div><table><tr><th>Host</th><th>Protocol</th><th>Hits</th></tr><tr><td>192.168.4.32</td><td>http</td><td>80</td></tr></table><table><tr><th>Destination</th><th>Protocol</th><th>Hits</th></tr><tr><td>192.168.4.74</td><td>smtp</td><td>42</td></tr></table></div>	Host	Protocol	Hits	192.168.4.32	http	80	Destination	Protocol	Hits	192.168.4.74	smtp	42	<p><a href="https://www.manageengine.com/products/firewall/firewall-virus-report.html">https://www.manageengine.com/products/firewall/firewall-virus-report.html</a></p>
Host	Protocol	Hits												
192.168.4.32	http	80												
Destination	Protocol	Hits												
192.168.4.74	smtp	42												
said computer program product is operable for use with at least one NOC server, a data warehouse, and an SDK for allowing access to the second information and at	<p>ManageEngine discloses that <i>said computer program product is operable for use with at least one NOC server, a data warehouse (e.g., the Central Vulnerability Database comprising a data storage warehouse to store global vulnerability information which is updated on time to time basis), and an SDK for allowing access to the second information and at least one of the plurality of techniques (e.g., the Central Vulnerability Database comprising patches for the remedies of the vulnerabilities that can be directly downloaded using the SDK files of the patches and incorporated on the devices to remove vulnerability);</i></p> <p>or</p>													

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

least one of the plurality of techniques; or

**Note:** See, for example, the evidence below (emphasis added, if any):


**Comprehensive vulnerability scanning**

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:


- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>


**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**




Latest Vulnerabilities




Microsoft Vulnerabilities




Third Party Vulnerabilities



Web Server Vulnerabilities



DB Server Vulnerabilities

 Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical


<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

	<p>Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64) <a href="#">← Back to list</a></p> <table border="1"> <tr> <td><b>Vulnerability Name</b></td><td>: Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)</td></tr> <tr> <td><b>Severity</b></td><td>: Important</td></tr> <tr> <td><b>Exploits</b></td><td>: Not available</td></tr> <tr> <td><b>CVE ID</b></td><td>: CVE-2024-4331,CVE-2024-4368</td></tr> <tr> <td><b>Solution</b></td><td>: <a href="#">MicrosoftEdgeEnterprise_124.0.2478.80_X64.msi</a></td></tr> <tr> <td><b>Published Date</b></td><td>: 03/05/2024</td></tr> <tr> <td><b>Updated Date</b></td><td>: 03/05/2024</td></tr> </table> <p><b>Disclaimer:</b> This webpage is intended to provide you information about vulnerability announcement for certain specific software products. The information is provided "As Is" without warranty of any kind. The links provided point to pages on the vendors websites. You can get more information by clicking the links to visit the relevant pages on the vendors website.</p> <p><a href="https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253712.html">https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253712.html</a></p>	<b>Vulnerability Name</b>	: Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	<b>Severity</b>	: Important	<b>Exploits</b>	: Not available	<b>CVE ID</b>	: CVE-2024-4331,CVE-2024-4368	<b>Solution</b>	: <a href="#">MicrosoftEdgeEnterprise_124.0.2478.80_X64.msi</a>	<b>Published Date</b>	: 03/05/2024	<b>Updated Date</b>	: 03/05/2024
<b>Vulnerability Name</b>	: Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)														
<b>Severity</b>	: Important														
<b>Exploits</b>	: Not available														
<b>CVE ID</b>	: CVE-2024-4331,CVE-2024-4368														
<b>Solution</b>	: <a href="#">MicrosoftEdgeEnterprise_124.0.2478.80_X64.msi</a>														
<b>Published Date</b>	: 03/05/2024														
<b>Updated Date</b>	: 03/05/2024														

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)

 [Back to list](#)

<b>Vulnerability Name</b>	:	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)
<b>Severity</b>	:	Critical
<b>Exploits</b>	:	Not available
<b>CVE ID</b>	:	CVE-2022-0778,CVE-2022-21712
<b>CVSS 3.0</b>	:	9.1 (I:N/AV:N/AC:L/S:U/PR:N/A:H/UI:N/C:H)
<b>Solution</b>	:	<a href="#">duoauthproxy-6.4.0.exe</a>
<b>Published Date</b>	:	03/05/2024
<b>Updated Date</b>	:	03/05/2024

**Disclaimer:** This webpage is intended to provide you information about vulnerability announcement for certain specific software products. The information is provided "As Is" without warranty of any kind. The links provided point to pages on the vendors websites. You can get more information by clicking the links to visit the relevant pages on the vendors website.

<https://www.manageengine.com/vulnerability-management/vulnerability-database/vmp-253706.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar contains a navigation menu with options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' It includes a search bar with the text 'Search by CVE ID: CVE-XXXX-XXXX' and a filter dropdown set to 'Threat Category'. Below this is a table with columns: Threats, Threat Category, Affected Systems, and Action. The table lists five entries, including Google Chrome (x64) and various Internet Explorer security updates. Each entry has a 'Fix' button in the Action column. At the bottom right of the table, it says '1 - 5 of 5' and '30'.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

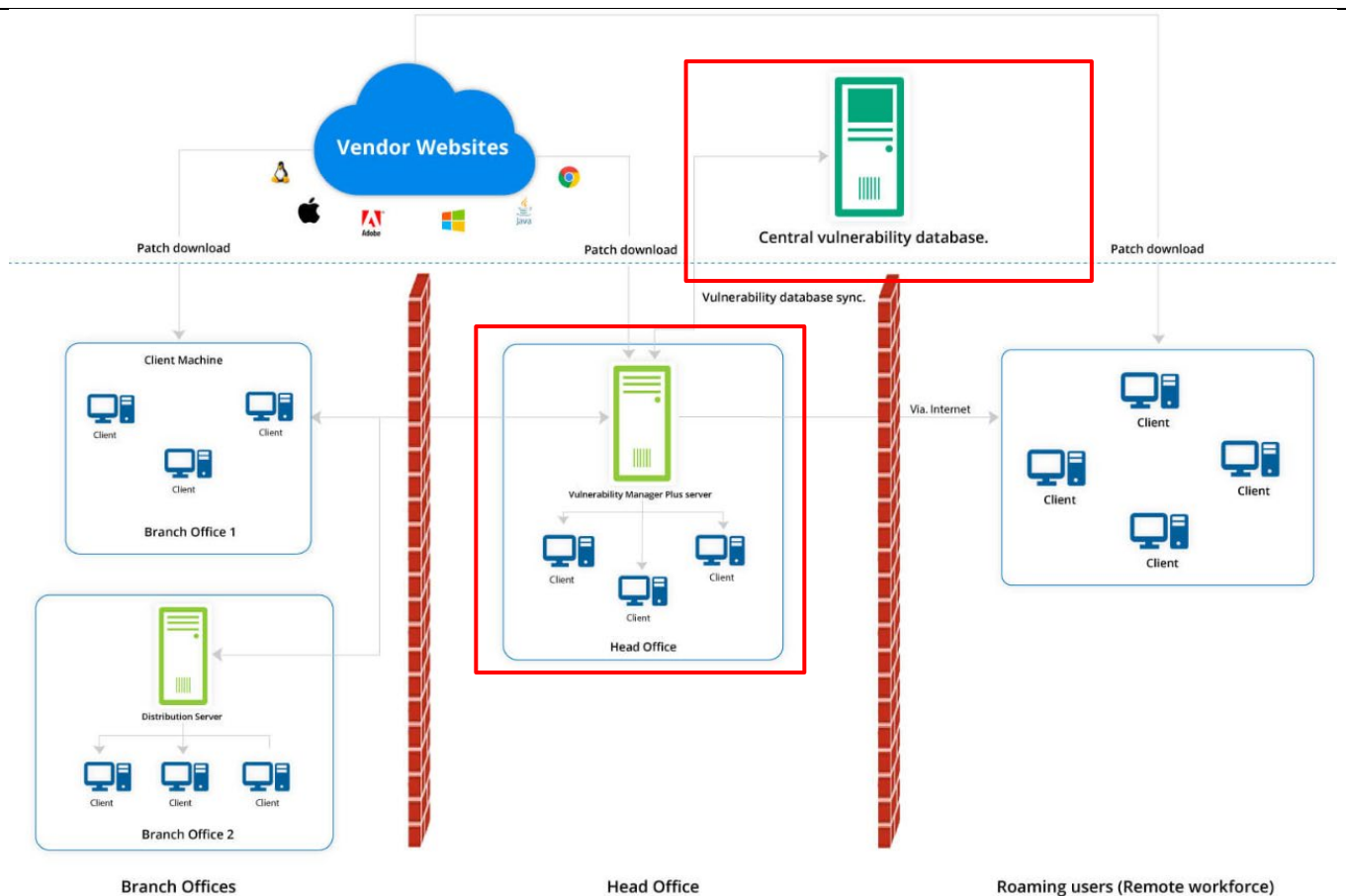
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****See what matters most at a glimpse with dashboard widgets**

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity  
Summary

Zero-day  
vulnerabilities

Vulnerability  
Age Matrix





Vulnerabilities  
Over Time

**High Priority  
Vulnerabilities**

**High Priority Vulnerabilities: Where your primary focus should be!**

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho**

said computer program product is operable such that said determination that the at least one networked device is actually vulnerable to the one or more actual vulnerabilities is carried out by directly querying a firmware or an operating system.

ManageEngine discloses that *said computer program product is operable such that said determination that the at least one networked device is actually vulnerable to the one or more actual vulnerabilities is carried out by directly querying a firmware or an operating system* (e.g., vulnerabilities on the network devices include software-based vulnerabilities like, end of life software, virus attack, malware attack, remote desktop sharing, etc. that are operated on the operating system of the devices including updates of the operating system).

**Note:** See, for example, the evidence below (emphasis added, if any):

## High risk software audit

The proliferation of devices and software has inevitably caused enterprises to serve as a home for a number of unsupported and unauthorized software. These software might bring a lot of security risks such as information disclosure, malicious code injection, unauthorized access that damages the organization's security and reputation. Take a brief look at the impacts of such software to your network.

<https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<p data-bbox="632 254 1138 293"><b>Dangers of high-risk software</b></p> <hr data-bbox="632 321 1633 328"/> <p data-bbox="632 358 915 389">  End of life software</p> <div data-bbox="617 427 1892 651" style="border: 2px solid red; padding: 10px;"><p data-bbox="632 435 1877 638">End of life software are rampant in enterprises due to lack of visibility and poor management. The consequences of running an end of life software outweighs its benefits. End of life OS and applications will not receive security updates from vendors to patch critical vulnerabilities, which makes them extremely vulnerable to exploits. Moreover, Legacy OSes can't run latest applications and they'll be stuck with legacy applications which will soon become end of life too, thus widening the attack surface. Also, businesses in regulated industries may also face significant fines for running out-of-date systems.</p></div> <p data-bbox="575 695 1715 727"><a href="https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html">https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html</a></p>
--	---

**EXHIBIT 15****U.S. Patent No 9,118,711 v. Zoho****| Peer to peer software**

P2P(Peer to Peer) applications such as Overnet, Morpheus, SoMud, GigaTribe allows a user to share and receive files over the internet. Files shared through Peer to Peer applications may be a pirated software, or copyrighted material which might land you in trouble for being involved in illegal actions. Also, the reliability of files shared through peer to peer software can't be verified which gives an attacker a leeway to transmit malicious code along with the file you download. Users might be unaware of what folders they are sharing which might allow unauthorized access to sensitive information stored in their computers. Some peer to peer applications may ask you to open certain ports on your firewall to transmit the files. This might allow an attacker to exploit the loopholes associated with the port or take advantage of any vulnerabilities that may exist in the peer to peer application.

**| Remote Desktop Sharing Software:**

IT employees often use remote desktop sharing software to facilitate remote access and management of remote server, virtual desktops, terminal servers, and applications over internet for the ease of operation. It's true that a remote desktop sharing software improves productivity, but it also increases the attack surface leaving an attacker to gain control over business critical assets once he finds a way to exploit the computer which is used to access them remotely. Also, if the remote desktop sharing sessions are not encrypted, it might increase the possibility of a Man-in-the-middle (MitM) attack.

<https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

	<h3>Audit and eliminate high-risk software in your network</h3> <hr/> <p>The above cited reasons explains the importance of auditing such high risk software that may be installed in network systems without the administrator's knowledge. With Vulnerability Manager Plus at your disposal, you can</p> <ul style="list-style-type: none"><li>• Monitor your network endpoints continuously and detect end of life softwares, peer to peer softwares and remote sharing tools present in them.</li><li>• Get details on the expiry date and the number of days before software in your network becomes end of life.</li><li>• Obtain real-time information on the number of machines that are affected by these software.</li><li>• Eliminate these software with just a click of a button from the console.</li></ul> <p><a href="https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html">https://www.manageengine.com/vulnerability-management/high-risk-software-audit.html</a></p>
--	--

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**How Vulnerability Manager Plus helps you fortify your network against zero-days and public disclosures?**

- Vulnerability Manager Plus includes a dedicated tab that displays zero-day and publicly disclosed vulnerabilities separately from other exploits so that you can instantly identify and respond to them.
- Generally, it takes two or more vulnerabilities to successfully launch a zero-day attack. With automated patching, you can stay current with the latest updates for all your OS and applications, thereby hampering the attacker's attempts.
- Vendors generally quickly publish work-arounds for public disclosures while they work on a fix. You can deploy these work-arounds to all the affected machines in an instant with Vulnerability Manager Plus' pre-built mitigation scripts.
- As long as your antivirus protection is up-to-date, you should be protected within a short time of a new zero-day threat. The antivirus audit feature enables you to sniff out endpoints with missing, disabled, or out-of-date antivirus programs. If your systems are running an outdated antivirus application, you can leverage Vulnerability Manager Plus' patch management feature to keep your antivirus up-to-date with the latest definition files.
- Your best bet against a zero-day threat is to harden the security of your IT ecosystem. Utilize the security configuration management feature to block vulnerable ports, disable legacy protocols, close insecure firewall connections, and disable unintended network shares with excessive permissions that usually serve as the vectors for malware to progress through the network laterally.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html?meseach>

**EXHIBIT 15**

**U.S. Patent No 9,118,711 v. Zoho**

**Case 3: End-of-life software**

The risks of running an end-of-life software outweighs its benefits. End-of-life software doesn't receive security updates from the vendor, and will remain forever vulnerable. A legacy OS often can't run the latest applications, meaning it is stuck with legacy applications, which will eventually reach end of life. Businesses in regulated industries may also face significant fines for running out-of-date systems. Vulnerability Manager Plus helps you keep track of which applications and OSs are approaching or have already reached end of life. Once they reach end of life, you can take further steps, like implementing compensation controls such as host or network based intrusion prevention systems, but it's recommended that you migrate to the latest version of the end-of-life software to eliminate the risks for once and all.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html?meseach>